TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk, FAX System and Data Security Kit Security Target

Version 1.00

October 13, 2021

KYOCERA Document Solutions Inc.

TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk, FAX System and Data Security Kit
Security Target

- History of Revisions-

Date	Version	Detail
2021-04-01	0.72	First release
2021-04-14	0.74	Modified for corresponding ORs.
2021-08-24	0.75	Modified for corresponding ORs.
2021-10-04	1.00	Update the version.

Table of Contents

List of Figures

List of Tables

TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk, FAX System and Data Security Kit
Security Target

1. ST Introduction

1.1. ST Reference

ST Title	TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk, FAX System and Data Security Kit
Security Target	
ST Version	1.00
Date	October 13, 2021
Author	KYOCERA Document Solutions Inc.

1.2. TOE Reference

TOE Title : TASKalfa 3554ci, TASKalfa 2554ci, TASKalfa 3554ciG, TASKalfa 2554ciG (KYOCERA), CS 3554ci, CS 2554ci(Copystar), 3508ci, 2508ci(TA Triumph-Adler/UTAX), with Hard Disk, FAX System and Data Security Kit

Remarks :
The models with Hard Disk, FAX System and Data Security Kit are the products that comprise the models such as TASKalfa 3554ci, TASKalfa 2554ci, TASKalfa 3554ciG, TASKalfa 2554ciG, CS 3554ci, CS 2554ci, 3508ci, 2508ci and the following additional options:

- Data Security Kit Option (Data Security Kit 10)
- Hard Disk Option (HD-15)
- FAX Option (FAX System 12)

TOE Version： System : 2XD_S000.002.266

FAX : 3R2_5100.003.012

Developer : KYOCERA Document Solutions Inc.

Applicable MFP : KYOCERA TASKalfa 3554ci, KYOCERA TASKalfa 2554ci,
KYOCERA TASKalfa 3554ciG, KYOCERA TASKalfa 2554ciG,
Copystar CS 3554ci, Copystar CS 2554ci,
TA Triumph-Adler 3508ci, TA Triumph-Adler 2508ci,
UTAX 3508ci, UTAX 2508ci

This TOE is identified by a combination of the respective MFP titles as listed in the TOE title and

each version of the two kinds of firmwares, which is installed on the above-described TOE. There are multiple MFP titles as listed above, however the MFP components are all the same. The only differences are print speed and sales destinations.

1.3. TOE Overview

1.3.1. TOE Type

The TOE defined in this ST is a Multi-Function Printer (MFP) manufactured by KYOCERA Document Solutions Inc., namely, "TASKalfa 3554ci, TASKalfa 2554ci, TASKalfa 3554ciG, TASKalfa 2554ciG, CS 3554ci, CS 2554ci, 3508ci, 2508ci", each of which includes mainly Copy function, Scan function, Print function, FAX function and Box function. As for the HDD, there are two HDD configurations depending on the sales area. One is equiped with HDD as standard and the other does is not equipped with an HDD. In the case the device is not equipped with an HDD, the optional HD-15 must be installed on the device to be available (Refer Section 1.4.1). As for the FAX function, optional FAX System 12 must be installed on the device to be available. As for the IPsec, optional Data Security Kit 10 must be installed on the device to be available.

1.3.2. TOE Usage

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

Figure 1-1 shows a normal user environment.

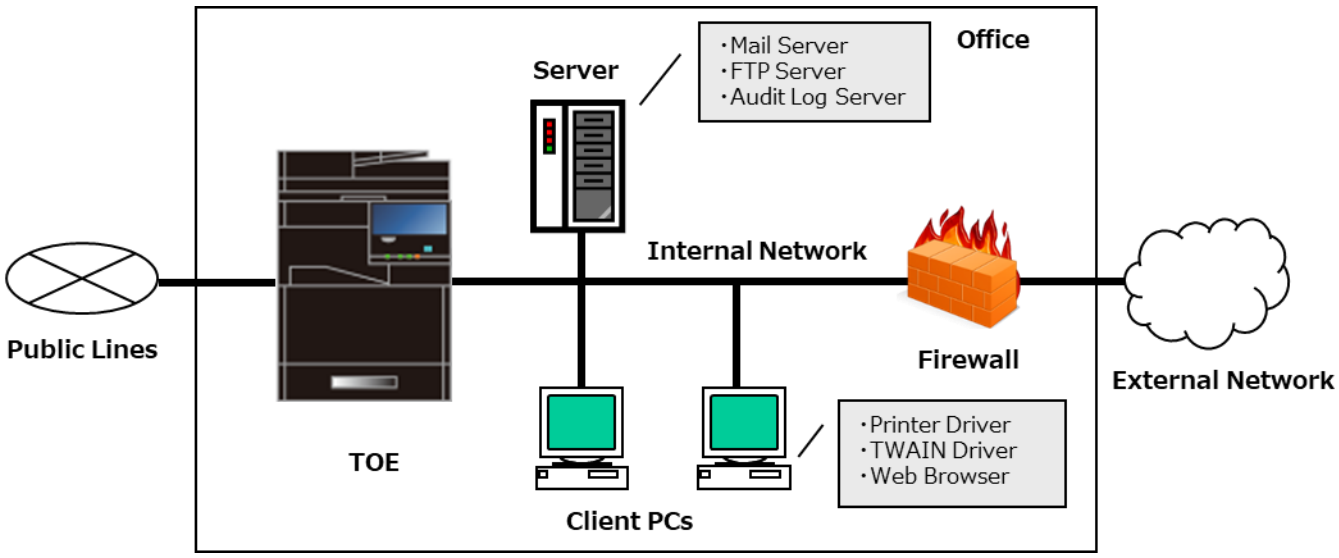

Figure 1-1 Common usage in the offices

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

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

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

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

1.3.3. Required Non-TOE Hardware, Software and Firmware

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

- Client PCs : IPsec(IKEv1) should be available.
  - Printer Driver : KX Driver
  - TWAIN Driver : Kyocera TWAIN Driver
  - Web Browser : Microsoft Internet Explorer 11.0
- Mail Server : IPsec(IKEv1) should be available.
- FTP Server : IPsec(IKEv1) should be available.
- Audit Log Server(syslog server) : IPsec(IKEv1) should be available.
- Cryptographic module : Kyocera MFP Cryptographic Module(A) should be available.
  - Hardware version : 2.1.10
  - CAVP Validation Number : C1892
- Cryptographic module for FDE : Kyocera MFP Cryptographic Module(A) – FDE should be available.
  - Hardware version : 2.3
  - CAVP Validation Number : C1933

1.3.4. Major Security Features of TOE

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

1.4. TOE Description

1.4.1. Physical Configuration of TOE

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

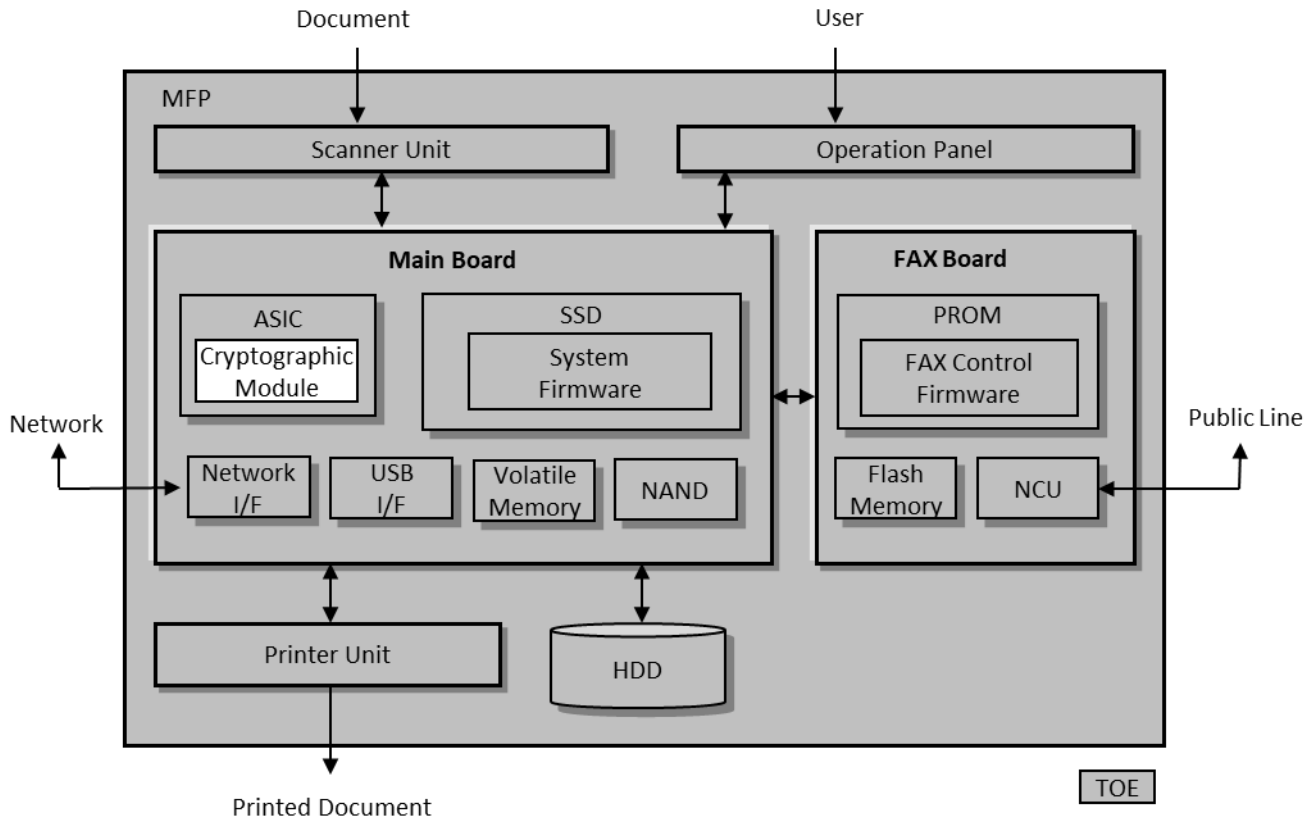

Figure 1-2 Physical Configuration of TOE

The TOE consists of an Operation Panel, a Scanner Unit, a Printer Unit, a Main Board, a FAX Board, HDD and SSD hardware, and firmwares.
The Operation Panel is the hardware that displays status and results upon receipt of input by the TOE user. The Scanner Unit and the Printer Unit are the hardware that input document into MFP and output as printed material.
A Main Board is the circuit board to control entire TOE. A system firmware is installed on a SSD, which is positioned on the Main Board. The Main Board has a Network Interface and a USB Interface.
The ASIC on the Main Board is installed with a cryptographic module to perform the HDD encryption function and Overwrite-Erase function(See below). A FIPS 140-2 certified cryptographic module, key derivation and entropy are provided by this cryptographic module in TOE environment.
A FAX control firmware that controls FAX communication is installed on the PROM, which is positioned on the FAX Board. Additionally, a FAX Board has a NCU as an interface.

As for memory mediums, a NAND that stores device settings, a Volatile Memory that is used as working area and a SSD for the system firmware installation are positioned on the Main Board. A

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

There are two kinds of HDD configurations on the MFP products depending on the sales area. One is equipped with HDD as standard and the other is not equipped with an HDD.

Table 1-1 MFP products and their HDD configurations

MFP product name	Sales Area	HDD Configuration
CS 3554ci, CS 2554ci	-	Installed as standard
TASKalfa 3554ci, TASKalfa 2554ci	North America	Installed as standard
	Other Area	Not installed
TASKalfa 3554ciG, TASKalfa 2554ciG, 3508ci, 2508ci	-	Not installed

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

Table 1-2 Delivery method for each TOE components

TOE Configuration	Form	Delivery Method	Identification Information
MFP Device (with HDD installed as standard)	MFP Device	Courier	MFP product name described in Table 1-1 MFP products and their HDD configurations and firmware version information described in TOE Reference + Mass storage device: HDD 320GB
MFP Device (without HDD)	MFP Device	Courier	MFP product name described in Table 1-1 MFP products and their HDD configurations and firmware version information described in TOE Reference + Mass storage device: Not installed
Hard Disk * If option installation is	HDD hardware	Courier	HD-15

required.			
Fax	FAX Board	Courier	FAX System 12
Guidance	Paper document, PDF format file in DVD	Included in the box of the MFP device.	Name and version described in Table 1-3.

* Firmware is preinstalled in the MFP

1.4.2. Logical Configuration of TOE

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

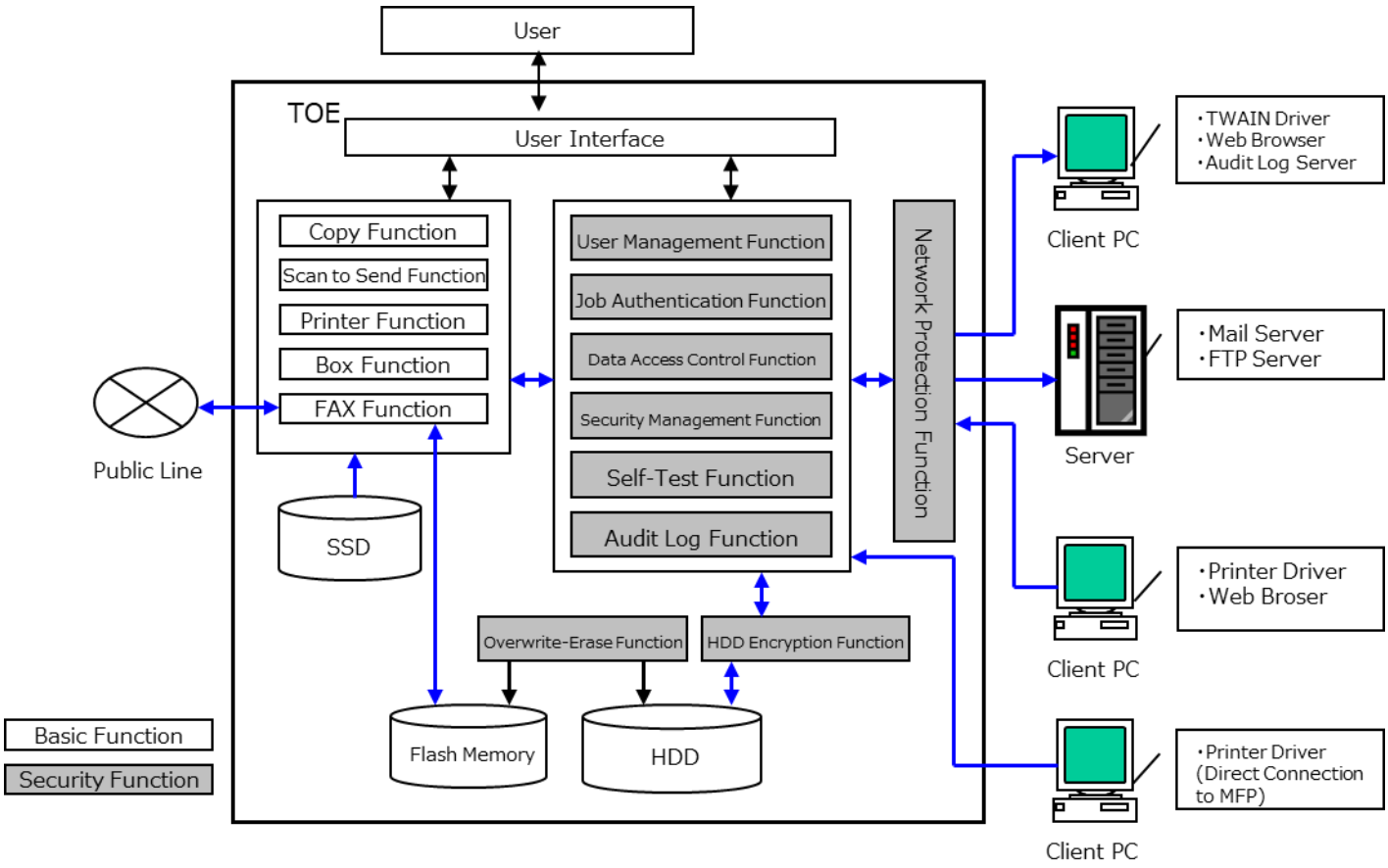

Figure 1-3 Logical Configuration of TOE

1.4.2.1. Basic Functions provided by TOE

The TOE provides the following basic functions.

- Copy Function

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

- Scan to Send Function

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

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

- Print Function

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

- Fax Function

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

- Box Function

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

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

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

- TWAIN send (TWAIN Driver)
- FAX send (Other faxes)
- USB Memory send (USB Memory)

1.4.2.2. Security Functions provided by TOE

TOE provides the following security functions. However, cryptographical primitives and entropy in HDD Encryption function and Network Protection Function(entropy only) are provided by the FIPS 140-2 Certified Cryptographic Module in TOE environment.

- User Management Function

  A function that identifies and authenticates users so that only authorized users can use the TOE. When using the TOE from the Operation Panel and Client PCs, a user will be required to enter his/her login user name and login user password for identification and authentication. The User Management Function includes a User Account Lockout Function, which prohibits the users access for a certain period of time if the number of identification and authentication attempts consecutively result in failure, a function, which protects feedback on input of login user password when performing identification and authentication and a function, which automatically logouts in case no operation has been done for a certain period of time.

- Data Access Control Function

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

- Job Authorization Function

  A function that restricts usage of the function so that only authorized persons can use basic functions of the TOE .
  The following types of Job Authorization are available.
  - Copy Job (Copy Function)
  - Print Job (Print Function)
  - Send Job (Scan to Send Function)
  - FAX Send Job (FAX Function)
  - FAX Reception Job (FAX Function)
  - Storing Job (Box Function)

- HDD Encryption Function

  A function that encrypts information assets stored in the HDD in order to prevent leakage of

data stored in the HDD inside the TOE.

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

- Audit Log Function
  A function that records and send to Audit Log server the audit logs of user operations and security-relevant events on the HDD. This function provides the audit trails of TOE use and security-relevant events. Stored audit logs can be accessed only by a device administrator.

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

- Trusted operation
  A function that verifies the authenticity of the firmware when updating the firmware of TOE. And a function that verifies the integrity of TSF executable code and TSF data to detect unauthorized alteration of the executable code of the TOE security functions.

- Network Protection Function
  A function that protects communication paths to prevent leaking and altering of data by eavesdropping of data in transition over the internal network connected to TOE.
  This function verifies the propriety of the destination to connect to and protects targeted information assets by encryption, when using a Scan to Send Function, a Print Function, a Box Function and a BOX Function from a Client PC (web browser), or a Security Management Function from a Client PC (web browser).

- PSTN Fax-Network Separation
  TOE ensure separation between the PSTN fax line and the Internal Network.

1.4.3. Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Maintenance Interface

1.4.4. Guidance

The guidance comprising the TOE is shown below.

Table 1-3 Guidance that comprises TOE

Name	Version
Notice (KYOCERA)	302XD5641002
Notice (Copystar)	302XD5642002
Notice (TA Triumph-Adler/UTAX)	302XD5643002
FAX System 12 Installation Guide	303RK5671101
TASKalfa 3554ci / TASKalfa 2554ci First Steps Quick Guide	302XC5602001
TASKalfa 2554ci / TASKalfa 3554ci / TASKalfa 4054ci / TASKalfa 5054ci / TASKalfa 6054ci / TASKalfa 7054ci Operation Guide	2XCKDEN000
TASKalfa 2554ci / TASKalfa 3554ci Safety Guide	302XC5622001
FAX System 12 Operation Guide	3RKKDEN300
Data Encryption/Overwrite Operation Guide	3MS2XCKDEN1
Command Center RX User Guide	CCRXKDEN23
TASKalfa 7054ci / TASKalfa 6054ci / TASKalfa 5054ci / TASKalfa 4054ci / TASKalfa 3554ci / TASKalfa 2554ci Printer Driver User Guide	2XCCLKTEN750.2020.02

2. Conformance Claim

2.1. CC Conformance Claim

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

CC version for which this ST and TOE claim conformance:

Common Criteria for Information Technology Security Evaluation
Part1: Introduction and general model Version 3.1 Revision 5
Part2: Security functional components Version 3.1 Revision 5
Part3: Security assurance components Version 3.1 Revision 5
Conformance of ST to CC part2: CC part2 Extended
Conformance of ST to CC part3: CC part3 Conformant

2.2. PP Conformance Claims

The PP to which this ST and TOE are conformant is as follows.

PP Name/Identification :	Protection Profile for Hardcopy Devices
PP Version :	1.0 dated September 10, 2015
Errata :	Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

2.3. Package Conformance Claims

The ST and TOE does not conform to the packages.

2.4. Conformance Rationale

The ST and TOE satisfy the following conditions required by PP and are "Exact Conformance" as required by PP. Therefore the TOE type is consistent with PP.

- Required Uses :

  Printing, Scanning, Copying, Network communications, Administration

- Conditionally Mandatory Uses :

  Storage and retrieval, Field-Replaceable Nonvolatile Storage

- Optional Uses :

  Image Overwrite, Purge Data

3. Security Problem Definitions

This section describes TOE users, Assets, Threats, Organizational Security Policies and Assumptions.

3.1. TOE user

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

Table 3-1 TOE User

Designation	Explanation
U.USER User	A person who is authorized to use the TOE.
U.NORMAL Normal User	A User who is identified and authenticated and do not have an administrative role.
U.ADMIN Administrator	An Administrator who is identified and authenticated and have an administrative role.

3.2. Assets

Protected Assets of TOE are User Data, TSF Data.

3.2.1. User Data

User Data is created by and for Users that do not affect the operation of the TSF. The User Data is composed of two types.

Table 3-2 User Data

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.

3.2.2. TSF Data

TSF Data is created by and for the TOE that might affect the operation of the TSF. The TSF Data is composed of two types.

Table 3-3 TSF Data

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.

TSF Data to be targeted by the TOE is shown in Table 3-4.

Table 3-4 TSF Data to be targeted by the TOE

Designation	TSF Data	Explanation
D.TSF.PROT	Login User Name	User's identification information that is used for the User Management Function.
	User Authorization	User's authorization information that is used for the User Management Function. There are authorization such as U. ADMINISTRATOR and U.NORMAL with respect to the TOE.
	Job Authorization Settings	This is to set whether or not the TOE attribute-based execution is authorized. Job authorization settings for the user management function are assigned to each user.
	Executable Attributes	Attributes that show Copy Function, Print Function, Scan to Send Function, FAX Function and Box Function of the TOE are excutable.
	Owner Information	Owner Information that targeted assets hold. Login user name is assigned to the owner information.
	Number of Retries until Locked (User Account Lockout Policy Settings)	Number of retries until user account is locked out. This information is used for the user management function.

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

3.3. Threats to TOE Assets

This section describes threats to assets described in clause 3.2.

Table 3-5 Threats

Threat	Description
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.

3.4. Organizational Security Policies for the TOE

Table 3-6 Organizational Security Policies for the TOE

Name	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	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	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	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.
P.PURGE_DATA	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.

3.5. Assumptions

Table 3-7 Assumptions for the TOE

Assumption	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.

4. Security Objectives

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

4.1. Security Objectives for the TOE

Security Objectives for the TOE is shown in .

Table 4-1 Security objectives for the operational environment

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.

Designation	Definition
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.

4.2. Security Objectives for the Operation Environment

Security Objectives for the operational environment is shown in .

Table 4-2 Security objectives for the 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.

Designation	Definition
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.

4.3. Security Objectives rationale

The relation among assumption, threat, and organizational security policy is shown in the table below.

Table 4-3 Security objectives rationale

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.

Threat/Policy/Assumption	Rationale
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.

5. Extended Components Definition

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

5.1. FAU_STG_EXT Extended: External Audit Trail Storages

Family behaviour:

This family defines requirements for the TSF to ensure that secure transmission of audit data from TOE to an External IT Entity.

Component leveling:

FAU_STG_EXT.1: Extended: External Audit Trail Storage	1

FAU_STG_EXT.1 External Audit Trail Storage requires the TSF to use a trusted channel implementing a secure protocol.

Management:

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

- The TSF shall have the ability to configure the cryptographic functionality.

Audit:

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

- There are no auditable events foreseen.

FAU_STG_EXT.1 Extended: Protected Audit Trail Storage

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.

Rationale:

The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.
This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

5.2. FCS_CKM_EXT Extended: Cryptographic Key Management

Family behaviour:
This family addresses the management aspects of cryptographic keys. Especially, this extended component is intended for cryptographic key destruction.

Component leveling:

FCS_CKM_EXT.4: Extended: Cryptographic Key Material Destruction	4

FCS_CKM_EXT.4 Cryptographic Key Material Destruction ensures not only keys but also key materials that are no longer needed are destroyed by using an approved method.

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
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.

Rationale:
Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.
This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.3. FCS_IPSEC_EXT Extended: IPsec selected

Family behaviour:
This family addresses requirements for protecting communications using IPsec.

Component leveling:

FCS_IPSEC_EXT.1 Extended: IPsec selected	1

FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

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

- There are no management actions foreseen.

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

- Failure to establish an IPsec SA.

FCS_IPSEC_EXT.1 Extended: IPsec selected
Hierarchical to: No other components.
Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

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

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection: tunnel mode, 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.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *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, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: *IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109*, [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers], and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

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

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on [*selection*: number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]; IKEv1 SA lifetimes can be established based on [*selection*: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: 24 *(2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP)),* [assignment: *other DH groups that are implemented by the TOE], no other DH groups*].

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

Rationale:

IPsec is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.4. FCS_KDF_EXT Extended: Cryptographic Key Derivation

Family behaviour:

This family specifies the means by which an intermediate key is derived from a specified set of submasks.

Component leveling:

FCS_KDF_EXT Cryptographic Key Derivation	1

FCS_KDF_EXT.1 Cryptographic Key Derivation requires the TSF to derive intermediate keys from submasks using the specified hash functions.

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

Hierarchical to: No other components.

Dependencies: FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication),
[if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

FCS_KDF_EXT.1.1 The TSF shall accept [selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*] to derive an intermediate key, as defined in [selection: *NIST SP 800-108* [selection: *KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132*], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

Rationale:
The TSF is required to specify the means by which an intermediate key is derived from a specified set of submasks using the specified hash functions.
This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key chains, and it is therefore placed in the FCS class with a single component.

5.5. FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family behaviour:
This family specifies the means by which an intermediate key is derived from a specified set of submasks.

Component leveling:

FCS_KYC_EXT Key Chaining	1

FCS_KYC_EXT Key Chaining, requires the TSF to maintain a key chain and specifies the characteristics of that chain.

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

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

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEVor DEK; intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s):* [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]] while maintaining an effective strength of [selection: *128 bits, 256 bits*].

Rationale:
Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain. However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

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

Family behaviour:
This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source.

Component leveling:

FCS_RBG_EXT.1 Extended: Random Bit Generation	1

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FCS_RBG_EXT.1 Extended: Random Bit Generation
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 [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] *software-based noise source(s)*, [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: *128 bits, 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.

Rationale:
Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.
This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.7. FDP_DSK_EXT Extended: Protection of Data on Disk

Family behaviour:
This family is to mandate the encryption of all protected data written to the storage.

Component leveling:

FDP_DSK_EXT.1 Extended: Protection of Data on Disk	1

FDP_DSK_EXT.1 Extended: Protection of Data on Disk, requires the TSF to encrypt all the Confidential TSF and User Data stored on the Field-Replaceable Nonvolatile Storage Devices in order to avoid storing these data in plaintext on the devices.

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

Hierarchical to: No other components.

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

FDP_DSK_EXT.1.1 The TSF shall [selection: *perform encryption in accordance with FCS_COP.1(d), use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

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

Rationale:

Extended: Protection of Data on Disk is to specify that encryption of any confidential data without user intervention, and the Common Criteria does not provide a suitable SFR for the Protection of Data on Disk.

This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

5.8. FDP_FXS_EXT Extended: Fax Separation

Family behaviour:

This family is to mandate the encryption of all protected data written to the storage.

Component leveling:

FDP_FXS_EXT.1 Extended: Fax Separation	1

FDP_FXS_EXT.1 Fax Separation, requires the fax interface cannot be used to create a network bridge between a PSTN and a LAN to which TOE is connected.

Management:

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

・ There are no management actions foreseen.

Audit:

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

・ There are no auditable events foreseen.

FDP_FXS_EXT.1 Extended: Fax 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.

Rationale:

Fax Separation is to protect a LAN against attack from PSTN line, and the Common Criteria does not provide a suitable SFR for the Protection of TSF or User Data.
This extended component protects the TSF Data or User Data, and it is therefore placed in the FDP class with a single component.

5.9. FIA_PMG_EXT Extended: Password Management

Family behaviour:

This family defines requirements for the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component leveling:

FIA_PMG_EXT.1 Extended: Password Management	1

FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management:

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

・ There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FIA_PMG_EXT.1 Extended: Password management

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: [selection: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"*, [assignment: *other characters*]];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater.

Rationale:

Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.

This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

5.10. FIA_PSK_EXT Extended: Pre-Shared Key Composition

Family behaviour:

This family defines requirements for the TSF to ensure the ability to use pre-shared keys for IPsec.

Component leveling:

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition	1

FIA_PSK_EXT.1 Pre-Shared Key Composition, ensures authenticity and access control for updates.

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
Hierarchical to: No other components.
Dependencies: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)..

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 [selection: [assignment: *other supported lengths], no other lengths*];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.1 The TSF shall condition the text-based pre-shared keys by using [selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] and be able to [selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*].

Rationale:
Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.
This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

5.11. FPT_KYP_EXT Extended: Protection of Key and Key Material

Family behaviour:

This family addresses the requirements for keys and key materials to be protected if and when written to nonvolatile storage.

Component leveling:

FPT_KYP_EXT.1 Protection of Key and Key Material	1

FPT_KYP_EXT.1 Extended: Protection of key and key material, requires the TSF to ensure that no plaintext key or key materials are written to nonvolatile storage.

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KYP_EXT.1.1 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, and not store any such plaintext key on a device that uses the key for its encryption.

Rationale:

Protection of Key and Key Material is to ensure that no plaintext key or key material are written to nonvolatile storage, and the Common Criteria does not provide a suitable SFR for the protection of key and key material.

This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

5.12. FPT_SKP_EXT Extended: Protection of TSF Data

Family behaviour:

This family addresses the requirements for managing and protecting the TSF data, such as cryptographic keys. This is a new family modelled as the FPT Class.

Component leveling:

FPT_SKP_EXT.1 Extended: Protection of TSF Data	1

FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_SKP_EXT.1 **Extended: Protection of TSF Data**
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.

Rationale:

Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.
This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.13. FPT_TST_EXT Extended: TSF testing

Family behaviour:

This family addresses the requirements for self-testing the TSF for selected correct operation.

Component leveling:

FPT_TST_EXT.1 Extended: TSF testing	1

FPT_TST_EXT.1 TSF testing requires a suite of self-testing to be run during initial start-up in order to demonstrate correct operation of the TSF.

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FPT_TST_EXT.1 **Extended: TSF testing**
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.

Rationale:
TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing. This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

5.14. FPT_TUD_EXT Extended: Trusted Update

Family behaviour:
This family defines requirements for the TSF to ensure that only administrators can update the TOE firmware/software, and that such firmware/software is authentic.

Component leveling:

FPT_TUD_EXT.1 Extended: Trusted Update	1

FPT_TUD_EXT.1 Trusted Update, ensures authenticity and access control for updates.

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update
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 [selection: published hash, no other functions] prior to installing those updates.

Rationale:
Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.
This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

6. Security Requirements

This section describes the TOE Security Functional Requirements.

6.1. TOE Security Functional Requirements.

6.1.1. Class FAU: Security Audit

	FAU_GEN.1	**Audit data generation** (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 6.1, [assignment: *other specifically defined auditable events*].

[assignment: *other specifically defined auditable events*]

- None

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 6-1,** [assignment: *other audit relevant information*].

[assignment: *other audit relevant information*]

- None

Table 6-1 Auditable data requirements

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
Failure to establish session	FTP_ITC.1 FTP_TRP.1(a) FTP_TRP.1(b)	Reason for failure

FAU_GEN.2 **User identify 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.

FAU_STG_EXT.1 **Extended: External Audi 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.

6.1.2. Class FCS: Cryptographic Support

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

Hierarchical to: No other components.
Dependencies: ~~[FCS_CKM.2 Cryptographic key distribution, or~~
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 [selection:**

- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite fieldbased key establishment schemes;***
- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curvebased key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")***
- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

[selection: *NIST Special …*]

- NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes;

FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(f) Cryptographic operation (Key Encyption)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_CKM.1.1(b) **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 [selection: 128 bit, 256 bit] that meet the following: No Standard.**

[selection: 128 bit, 256 bit]

- 128bit
- 256bit

FCS_CKM_EXT.4 **Extended: Cryptographic Key Material Destruction**
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

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.

FCS_CKM.4 **Cryptographic Key Destruction**
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

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 [selection:

- **For volatile memory, the destruction shall be executed by [selection:** *powering off a device,* **[assignment:** *other mechanism that ensures keys are destroyed***]].**
- **For nonvolatile storage, the destruction shall be executed by a [selection:** *single, three or more times***] overwrite of key data storage location consisting of [selection:** *a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern***], followed by a [selection:** *read-verify, none***]. If read-verification of the overwritten data fails, the process shall be repeated again;.**

] that meets the following: [**selection**: *NIST SP800-88, no standard*].

[selection: For volatile memory…]

- **For volatile memory, the destruction shall be executed by [selection:** *powering off a device,* **[assignment:** *other mechanism that ensures keys are destroyed***]].**
- **For nonvolatile storage, the destruction shall be executed by a [selection:** *single, three or more times***] overwrite of key data storage location consisting of [selection:** *a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern***], followed by a [selection:** *read-verify, none***]. If read-verification of the overwritten data fails, the process shall be repeated again;.**

[selection: *powering off a device,* **[assignment:** *other mechanism that ensures keys are destroyed***]**]

- powering off a device

[selection: *single, three or more times*]

- single

[selection: *a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern*]

- a static pattern

[selection: *read-verify, none*]

- none

[selection: *NIST SP800-88, no standard*]

- no standard

FCS_COP.1(a)	**Cryptographic operation (Symmetric encryption/decryption)** (for O.COMMS_PROTECTION)

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(a) **Refinement:** The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [assignment:** *one or more modes*] and cryptographic key sizes **128-bits and 256-bits** that meets the following:

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

[assignment: *one or more modes*]

- CBC

[selection: *NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*]

- NIST SP 800-38A

	FCS_COP.1(b)	**Cryptographic operation (for signature gerenation/verification)** (for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

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(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 [selection:

- *Digital Signature Algorithm (DSA) with key sizes (modulus) of* [**assignment:** *2048 bits or greater*],
- *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of* [**assignment:** *2048 bits or greater*], *or*
- *Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of* [**assignment:** *256 bits or greater*]]

that meets the following: [**selection**:

Case: Digital Signature Algorithm

- *FIPS PUB 186-4, "Digital Signature Standard"*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-4, "Digital Signature Standard"*

Case: Elliptic Curve Digital Signature Algorithm

FIPS PUB 186-4, "Digital Signature Standard"

- *The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").*

].

[selection: *Digital Signature …*]

- *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of* [**assignment:** *2048 bits or greater*], *or*

[assignment: *2048 bits or greater*]

- 2048 bits

[selection: *Case: Digital …*]

- FIPS PUB 186-4, "Digital Signature Standard"

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
(for O.STORAGE_ENCRYPTION, O.COMMS_PROTECTION)

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

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

[selection: *ISO/IEC 18031:2011, NIST SP 800-90A*]

- NIST SP 800-90A

[selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*]

- CTR_DRBG (AES)

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] *software-based noise source(s)*, [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: *128 bits, 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.

[selection: [assignment: *number of software-based sources*] *software-based noise*

source(s), [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: *128 bits, 256 bits*]

- [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: *128 bits, 256 bits*]

[assignment: *number of hardware-based sources*]

- 8

[selection: *128 bits, 256 bits*]

- 256 bit

6.1.3. Class FDP: User Data Protection

	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 6-2 and Table 6-3.**

	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 initialisation

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 6-2 and Table 6-3.**

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 6-2 and Table 6-3.*

FDP_ ACF.1.3 **Refinement:** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*]

- None

FDP_ ACF.1.4 **Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules t****hat do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules t****hat do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*]

- None

Table 6-2 D.USER.DOC Access Control SFP

		Create	Read	Modify	Delete
Print	Operation:	*Submit a document to be printed*	*View image or Release printed output*	*Modify stored document*	*Delete stored document*
	Job owner	(note 1)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied
Scan	Operation:	*Submit a document for scanning*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)	denied	denied	
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied
Copy	Operation:	*Submit a document for*	*View scanned image or*	*Modify stored image*	*Delete stored image*

		copying	*Release printed copy output*		
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied
Fax send	Operation:	*Submit a document to send as a fax*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)	denied	denied	
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied
Fax receive	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*
	Job owner	(note 3)		denied	
	U.ADMIN	(note 4)		denied	
	U.NORMAL	(note 4)	denied	denied	Denied
	Unauthenticated		denied	denied	Denied
Storage / retrieval	Operation:	*Store document*	*Retrieve stored document*	*Modify stored document*	*Delete stored document*
	Job owner	(note 1)			
	U.ADMIN	denied			
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied

Table 6-3 D.USER.JOB Access Control SFP

		Create	Read	Modify	Delete
Print	Operation:	*Create print job*	*View print queue / log*	*Modify print job*	*Cancel print job*
	Job owner	(note 1)		denied	
	U.ADMIN	denied		denied	

	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied
Scan	Operation:	*Create scan job*	*View scan status / log*	*Modify scan job*	*Cancel scan job*
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied
Copy	Operation:	*Create copy job*	*View copy status / log*	*Modify copy job*	*Cancel copy job*
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied
Fax send	Operation:	*Create fax send job*	*View fax job queue / log*	*Modify fax send job*	*Cancel fax send job*
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied
Fax receive	Operation:	*Create fax receive job*	*View fax receive status / log*	*Modify fax receive job*	*Cancel fax receive job*
	Job owner	(note 3)		denied	
	U.ADMIN	(note 4)		denied	
	U.NORMAL	(note 4)	denied	denied	Denied
	Unauthenticated		denied	denied	Denied
Storage / retrieval	Operation:	*Create storage / retrieval job*	*View storage / retrieval log*	*Modify storage / retrieval job*	*Cancel storage / retrieval job*
	Job owner	(note 1)			
	U.ADMIN	denied			
	U.NORMAL		denied	denied	Denied
	Unauthenticated	denied	denied	denied	Denied

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.

6.1.4. Class FIA: Identification and Authentication

	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 [selection: [assignment: *positive integer number],* an administrator configurable positive integer within [assignment: *range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

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

- an administrator configurable positive integer within [assignment: range of acceptable values]

[assignment: range of acceptable values]

- 1 to 10

[assignment: *list of authentication events*]

- Consecutive unsuccessful authentication attempts since the last successful authentication occur related to login user name designated by login from an operational panel.
- Consecutive unsuccessful authentication attempts since the last successful authentication occur related to login user name designated by login from a client PC.

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

[selection: *met, surpassed*]

- met

[assignment: *list of actions*]

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

	FIA_ATD.1	**User attribute definition** (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: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]

- Login User Name, User Authorization, Job Authorization Setting

	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: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: *other characters*]];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

[selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: *other characters*]]

- “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” and [assignment: *other characters*]

[assignment: *other characters*]

- "-", "¥", "[", "]", ":", ";", ",", ".", "/", "@", "\", "=", "~", "|", "^", "{", "}", "+", "<", ">", "?", "_"

	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 [assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is authenticated.

[assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***]

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

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

	FIA_UAU.7	**Protected authentication feedback** (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 [assignment: *list of feedback*] to the user while the authentication is in progress.

[assignment: *list of feedback*]

- dummy characters（*：asterisk）

	FIA_UID.1	**Timing of identification** (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 [assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is identified.

[assignment: *list of TSF-mediated actions* ***thatdo not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***]

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

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

	FIA_USB.1	**User-subject binding** (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: [assignment: *list of user security attributes*].

[assignment: *list of user security attributes*]

- Login User Name, User Authorization, Job Authorization Setting

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

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

- None

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

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

- None

6.1.5. Class FMT: Security Management

FMT_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 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to **U.ADMIN**.

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

- modify the behaviour of

[assignment: *list of functions*]

- Auditing
- User Authentication
- Storage Data Encryption
- Firmware update

- Trusted Commnunication

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, ~~or~~
~~FDP_IFC.1 Subset information flow 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 in Table 6-2** to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[selection: *change_default, query, modify, delete, [assignment: other operations]*]
- Operation(s) as listed in Table 6-4

[assignment: *list of security attributes*]
- Security Attributes as listed in Table 6-4

[assignment: *the authorised identified roles*]
- Role as listed in Table 6-4

Table 6-4 Management of security attributes

Security Attributes	Operation(s)	Authorised Roles
Box Owner	query, modify	U.ADMINISTRATOR
Box Permission	query, modify	U.ADMINISTRATOR
		U.NORMAL that matches a Box Owner.
Owner Information	query, modify	U.ADMINISTRATOR

FMT_MSA.3	**Static attribute initialisation** (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 in Table 6-2** to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

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

- restrictive

FMT_MSA.3.2 Refinement: The TSF shall allow the [selection: *U.ADMIN, no role*] to specify alternative initial values to override the default values when an object or information is created.

[selection: *U.ADMIN, no role*]

- no role

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 6-5, Table 6-6.

Table 6-5 Operation of TSF data

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

Table 6-6 Operation of TSF data

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

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 Refinement: The TSF shall be capable of performing the following management functions: [assignment: *list of management functions provided by the TSF*].

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

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

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.

6.1.6. Class FPT: TSF Protection

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.

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.

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.

FPT_TUD_EXP.1 **Extended: Trusted Update**
(for O. UPDATE_VERIFICATION)

Hierarchical to: No other components.
Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
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 [selection: *published hash, no other functions*] prior to installing those updates.

[selection: *published hash, no other functions*]

- no other functions

6.1.7. Class FTA: TOE Access

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

[assignment: *time interval of user inactivity*]

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

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

6.1.8. Class FTP: High Trusted Path/Channel

	FTP_ITC.1	**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 Refinement: The TSF shall **use [selection: *IPsec, SSH, TLS, TLS/HTTPS*] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: [selection:** *authentication server, [assignment: other capabilities]*] 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.**

[selection: ***IPsec, SSH, TLS, TLS/HTTPS***]
- IPsec

[selection: *authentication server, [assignment: other capabilities]*]
- [assignment: other capabilities]

[assignment: *other capabilities*]
- FTP Servr
- SMTP Server
- Audi Log Server

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

FTP_ITC.1.3 Refinement: The TSF shall initiate communication via the trusted channel for [assignment: *list of services for which the TSF is able to initiate communications*].

[assignment: *list of services for which the TSF is able to initiate communications*]
- FTP Service
- E-mail Service
- Audit Log Service

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 [selection, choose at least one of: IPsec, SSH, TLS, 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.

[selection, choose at least one of: ***IPsec, SSH, TLS, TLS/HTTPS***]

- IPsec

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.**

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 [selection, choose at least one of: IPsec, SSH, TLS, 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.**

[selection, choose at least one of: ***IPsec, SSH, TLS, TLS/HTTPS***]

- IPsec

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

[selection: **the TSF, remote users**]

- remote users

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.**

< Appendix B.1: Conditionally Mandatory Requirements (Confidential Data on Field-Replaceable Nonvolatile Storage Devices) >

6.1.9. Class FPT: Protection of the TSF

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.

6.1.10. Class FCS: Cryptographic support

FCS_KYC_EXT.1	**Extended: Key Chaining** (for O.STORAGE_EXCRYPTION)

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)]

FCS_KYC_EXT.1.1: The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEV or DEK; intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s):* [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]] while maintaining an effective strength of [selection: *128 bits, 256 bits*].

[selection: *one, using a submask as the BEV or DEK; intermediate …*]

- intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s): [selection: key wrapping as specified in FCS_COP.1(e), key

combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)]

[selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]

- key derivation as specified in FCS_KDF_EXT.1

[selection: *128 bits, 256 bits*]

- 256bit

6.1.11. Class FDP: User data protection

FDP_DSK_EXT.1 Extended: Protection of Data on Disk
(for O.STORAGE_EXCRYPTION)

Hierarchical to: No other components.
Dependencies: FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption).

FDP_DSK_EXT.1.1: The TSF shall [selection: *perform encryption in accordance with FCS_COP.1(d) , use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*], such that any **Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext Confidential TSF Data.**

[selection: *perform encryption in accordance with FCS_COP.1(d) , use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*]

- perform encryption in accordance with FCS_COP.1(d)

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

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.

< Appendix C: Optional Requirements (C.2 Image Overwrite) >

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.

< Appendix D: Selection-based Requirements (D.1 Confidential Data on Field-Replaceable Nonvolatile Storage Devices) >

6.1.12. Class FCS: Cryptographic support

FCS_COP.1(d)	**Cryptographic operation (AES Data Encryption/Decryption)** (for O.STORAGE_EXCRYPTION)

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(d): The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [selection: *CBC, GCM, XTS*] mode** and cryptographic key sizes [selection: *128 bits, 256 bits*] that meet the following: **AES as specified in ISO/IEC 18033-3, [selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772, and XTS as specified in IEEE 1619*].**

[selection: *CBC, GCM, XTS*]
- XTS

[selection: *128 bits, 256 bits*]
- 256bit

[selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772, and XTS as specified in IEEE 1619*]
- XTS as specified in IEEE 1619

< Appendix D: Selection-based Requirements (D.2 Protected Communications) >

6.1.13. Class FCS: Cryptographic support

FCS_IPSEC_EXT.1 Extended: IPsec selected
(selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to: No other components.
Dependencies: ~~FPT_ITT.1 Basic internal TSF data transfer protection,~~
FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

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

FCS_IPSEC_EXT.1.2: The TSF shall implement [selection: *tunnel mode, transport mode*].

[selection: *tunnel mode, transport mode*]
- 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.

FCS_IPSEC_EXT.1.4: The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *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, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*].

[selection: *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, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*]

- 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

FCS_IPSEC_EXT.1.5: The TSF shall implement the protocol: [selection: *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109,* [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996, [selection: with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].

[selection: *IKEv1 as defined…; IKEv2 as defined…*]

- IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers], and [selection: no other RFCs for hash functions, RFC 4868 for hash functions*]

[selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*]

- no other RFCs for extended sequence numbers

[selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]

- RFC 4868 for hash functions

FCS_IPSEC_EXT.1.6: The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other*

algorithm].

[selection: *IKEv1, IKEv2*]

- IKEv1

[selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*]

- no other algorithm

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

FCS_IPSEC_EXT.1.8: The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on* [selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]; *IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

[selection: *IKEv2 SA lifetimes can be established based on* [selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]; *IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]]

- *IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]

[selection: *number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]

- length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs

FCS_IPSEC_EXT.1.9: The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP)),* [assignment: *other DH groups that are implemented by the TOE], no other DH groups*].

[selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-*

bit Random ECP, 5 (1536-bit MODP)), [assignment: *other DH groups that are implemented by the TOE], no other DH groups*]

- no other DH groups

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

[selection: *RSA, ECDSA*]

- RSA

6.1.14. Class FCS: Cryptographic support

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 HMAC-[selection: *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*], key size [assignment: *key size (in bits) used in HMAC*], and message digest sizes [selection: *160, 224, 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.”

[selection: *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*]

- SHA-1, SHA-256

[assignment: *key size (in bits) used in HMAC*]

- 160, 256 bit

[selection: *160, 224, 256, 384, 512*]

- 160, 256

6.1.15. Class FIA: Identification and authentication

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)

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 [selection: [assignment: *other supported lengths], no other lengths*];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

[selection: [assignment: *other supported lengths], no other lengths*]

- [assignment: *other supported lengths]*

[assignment: *other supported lengths*]

- 1-128

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] and be able to [selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*].

[selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]]

- SHA-1, SHA-256

[assignment: *method of conditioning text string*]]

- none

[selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*]

- use no other pre-shared keys

< Appendix D: Selection-based Requirements (D.3 Trusted Update) >

6.1.16. Class FCS: Cryptographic support

FCS_COP.1(c)	**Cryptgraphic 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) Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [selection: *SHA-1, SHA-256, SHA-384, SHA-512*] that meet the following: [**ISO/IEC 10118-3:2004**].

[selection: *SHA-1, SHA-256, SHA-384, SHA-512*]

- Listed in Table 6-7

Table 6-7 Cryptographic hashing setvices

Usage	Hashing services
IPsec IKEv1 Authentication algorithm	SHA-1, SHA-256
Key Derivation	SHA-256
Signature verification of firmware	SHA-256

< Appendix D: Selection-based Requirements (D.4 Passphrase-based Key Entry) >

6.1.17. Class FCS: Cryptographic support

FCS_KDF_EXT.1	**Extended: Cryptographic Key Derivation** (for O. STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication),
[if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

FCS_KDF_EXT.1.1 The TSF shall accept [selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*] to derive an intermediate key, as defined in [selection: *NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132*], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

[selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*]

- a RNG generated submask as specified in FCS_RBG_EXT.1

[selection: *NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132*]

- NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode]

[selection: *KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode*]

- KDF in Feedback Mode

FCS_COP.1(h)	**Cryptographic Operation (for keyed-hash message authentication)** (selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)

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_COP.1(c) Cryptographic operation (Hash Algorithm),
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(h) Refinement: The TSF shall perform [**keyed-hash message authentication**] in

accordance with [**selection**: *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512*] and cryptographic key sizes [assignment: *key size (in bits) used in HMAC*] that meet the following: [**ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"; ISO/IEC 10118**].

[selection: *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512*]

- HMAC-SHA-256

[assignment: *key size (in bits) used in HMAC*]

- 256bit

6.2. TOE Security Assurance Requirement

Security Assurance Requirements (SARs) are described in **Table 6-8 TOE Security Assurance Requirements**.

Table 6-8 TOE Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

6.3. Security Requirements Rationale

6.3.1. Dependency Relationship of the TOE Security Functional Requirements

Table 6-9 shows the dependency relationship of the TOE security functional requirements.

Table 6-9 The dependency of the TOE Security Functional Requirements

Functional Requirements	Dependency Relationship by PP	Dependency Relationship by ST	Dependencies Not Satisfied
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	N/A
FAU_STG_EXT.1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1	N/A
FCS_CKM.1(a)	[FCS_COP.1(b)], FCS_CKM_EXT.4	[FCS_COP.1(b)], FCS_CKM_EXT.4	N/A
FCS_CKM.1(b)	[FCS_COP.1(f)], FCS_CKM_EXT.4, FCS_RBG_EXT.1	FCS_CKM_EXT.4, FCS_RBG_EXT.1	N/A
FCS_CKM_EXT.4	[FCS_CKM.1(a), or FCS_CKM.1(b)], FCS_CKM.4	[FCS_CKM.1(a), or FCS_CKM.1(b)], FCS_CKM.4	N/A
FCS_CKM.4	[FCS_CKM.1(a), or FCS_CKM.1(b)]	[FCS_CKM.1(a), or FCS_CKM.1(b)]	N/A
FCS_COP.1(a)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	[FCS_CKM.1(b)], FCS_CKM_EXT.4	N/A
FCS_COP.1(b)	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
FCS_RBG_EXT.1	No dependenceies	No dependenceies	N/A
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	N/A
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	N/A
FIA_ATD.1	No dependencies.	No dependencies.	N/A
FIA_PMG_EXT.1	No dependencies.	No dependencies.	N/A
FIA_UAU.1	FIA_UID.1	FIA_UID.1	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	N/A
FIA_UID.1	No dependencies.	No dependencies.	N/A
FIA_USB.1	FIA_ATD.1.	FIA_ATD.1.	N/A
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A

FMT_MSA.1	[FDP_ACC.1] FMT_SMR.1 FMT_SMF.1	[FDP_ACC.1] FMT_SMR.1 FMT_SMF.1	N/A
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	N/A
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A
FMT_SMF.1	No dependencies.	No dependencies.	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1	N/A
FPT_SKP_EXT.1	No dependencies.	No dependencies.	N/A
FPT_STM.1	No dependencies.	No dependencies.	N/A
FPT_TST_EXT.1	No dependencies.	No dependencies.	N/A
FPT_TUD_EXP.1	FCS_COP.1(b) FCS_COP.1(c)	FCS_COP.1(b) FCS_COP.1(c)	N/A
FTA_SSL.3	No dependencies.	No dependencies.	N/A
FTP_ITC.1	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A
FTP_TRP.1(b)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A
FPT_KYP_EXT.1	No dependencies.	No dependencies.	N/A
FCS_KYC_EXT.1	[FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(f), FCS_KDF_EXT.1, FCS_COP.1(i)]	FCS_KDF_EXT.1	N/A
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	N/A
FDP_FXS_EXT.1	No dependencies.	No dependencies.	N/A
FDP_RIP.1(a)	No dependencies.	No dependencies.	N/A
FCS_COP.1(d)	[FCS_CKM.1(b)] FCS_CKM_EXT.4	[FCS_CKM.1(b)] FCS_CKM_EXT.4	N/A
FCS_IPSEC_EXT.1	FIA_PSK_EXT.1	FIA_PSK_EXT.1	N/A

	FCS_COP.1(g)	FCS_COP.1(g)	
FCS_COP.1(g)	[FCS_CKM.1(b)] FCS_CKM_EXT.4	[FCS_CKM.1(b)] FCS_CKM_EXT.4	N/A
FIA_PSK_EXT.1	FCS_RBG_EXT.1	FCS_RBG_EXT.1	N/A
FCS_COP.1(c)	No dependencies.	No dependencies.	N/A
FCS_KDF_EXT.1	FCS_COP.1(h) FCS_RBG_EXT.1	FCS_COP.1(h) FCS_RBG_EXT.1	N/A
FCS_COP.1(h)	[FCS_CKM.1(b)] FCS_COP.1(c) FCS_CKM_EXT.4	[FCS_CKM.1(b)] FCS_COP.1(c) FCS_CKM_EXT.4	N/A

6.3.2. Security Assurance Requirements Rationale

The SAR that this ST insists on completely corresponds with the SAR that PP prescribes.

7. TOE Summary Specification

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

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

Table 7-1 TOE security functions and security functional requirements

Security Functions / Functional Requirements	User Management Function	Data Access Control Function	Job Authorization Function	HDD Encryption Function	Overwrite-Erase Function	Audit Log Function	Security Management Function	Trusted operation	Network Protection Function	PSTN Fax-Network Separation
FAU_GEN.1						✓				
FAU_GEN.2						✓				
FAU_STG_EXT.1						✓				
FCS_CKM.1(a)									✓	
FCS_CKM.1(b)				✓					✓	
FCS_CKM_EXT.4				✓					✓	
FCS_CKM.4				✓					✓	
FCS_COP.1(a)									✓	
FCS_COP.1(b)								✓	✓	
FCS_RBG_EXT.1				✓					✓	
FDP_ACC.1		✓	✓							
FDP_ACF.1		✓	✓							
FIA_AFL.1	✓									
FIA_ATD.1	✓									
FIA_PMG_EXT.1	✓									
FIA_UAU.1	✓									
FIA_UAU.7	✓									
FIA_UID.1	✓									
FIA_USB.1	✓									
FMT_MOF.1							✓			

FMT_MSA.1							✓			
FMT_MSA.3		✓	✓							
FMT_MTD.1							✓			
FMT_SMF.1							✓			
FMT_SMR.1							✓			
FPT_SKP_EXT.1									✓	
FPT_STM.1						✓				
FPT_TST_EXT.1								✓		
FPT_TUD_EXP.1								✓		
FTA_SSL.3	✓									
FTP_ITC.1						✓			✓	
FTP_TRP.1(a)									✓	
FTP_TRP.1(b)									✓	
FPT_KYP_EXT.1				✓						
FCS_KYC_EXT.1				✓						
FDP_DSK_EXT.1				✓						
FDP_FXS_EXT.1										✓
FDP_RIP.1(a)					✓					
FCS_COP.1(d)				✓						
FCS_IPSEC_EXT.1									✓	
FCS_COP.1(g)									✓	
FIA_PSK_EXT.1									✓	
FCS_COP.1(c)				✓				✓	✓	
FCS_KDF_EXT.1				✓						
FCS_COP.1(h)				✓						

7.1. User Management Function

User management function is a function that identifies and authenticates whether persons are authorized users when users intend to operate the TOE from the operation panel or the client PCs. For identification authentication, TOE obtains the login user name and login password from the user, performs identification authentication using the local authentication method, and permits the operation of TOE only to users who are determined to be authorized users as a result of verification.

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

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

password obtained from a user job.

(1) FIA_AFL.1 Authentication failure handling

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

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

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

(2) FIA_ATD.1 User attribute definition

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

(3) FIA_PMG_EXT.1 Password Management

The TOE can set the password of U.USER to a string that is a combination of uppercase and lowercase letters, numbers, and the following special characters:

“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “-”, “¥”, “[”, “]”, “:”, “;”, “,”, “.”, “/“, “\”, “`”, “=”, “~”, “|”, “`”, “{”, “}”, “+”, “<”, “>“, “?”, “_”

The U.ADMIN can also set a minimum password length of 0 ~ 64 characters. Therefore, the TOE can be limited to more than 15 characters by this setting.

(4) FIA_UID.1 Timing of identification

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

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

(5) FIA_UAU.1 Timing of authentication

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

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

(6) FIA_UAU.7 Protected authentication feedback

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

(7) FIA_USB.1 User-subject biding

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

(8) FTA_SSL.3 TSF-initiated termination

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

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

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

7.2. Data Access Control Function

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

(1) FDP_ACC.1 Subset access control

FDP_ACF.1 Secuirty attribute based access control

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

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

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

Targeted Assets	Operations	Users	Access Control Rules
Image Data	Box Print (Job after print	Normal User	It is allowed for a normal user to

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

			image data.

(2) FMT_MSA.3 Static attribute initialization

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

7.3. Job Authorization Function

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

(1) FDP_ACC.1 Subset access control

FDP_ACF.1 Security attribute-based access control

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

Table 7-3 Access Control Rules for Job Authorization Function

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

(2) FMT_MSA.3 Static attribute initialization

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

7.4. HDD Encryption Function

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

(1) FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)
FCS_KYC_EXT.1 Extended: Key Chaining
FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation
FCS_COP.1(c) Cryptgraphic operation (Hash Algorithm)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)
FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

The TOE generates an encryption key for use in encrypting HDD by key derivation function(KDF) in accordance with NIST SP800-108 by using Cryptographic Module. The encryption key size is 256bits. Encryption key is derived from the Salt and IV and KDK. Salt is obtained a RNG generated submask as specified in FCS_RBG_EXT.1 using Cryptographic Module, and KDK uses a unique value for each Hardware. A unique value for each Hardware is stored within Cryptographic Module and cannot be retrieved or rewritten. KDF uses feedback mode and PRF is HMAC-SHA-256(Use SHA-256 in accordance with FCS_COP.1(c)). The block size is 64 bytes, and the output MAC length is 256 bits.
Encryption algorithms used in KDF are shown in Table 7-4.
Note that key generation is provided by the FIPS 140-2 Certified Cryptographic Module in TOE environment.(CAVP Validation Number : C1892)

Table 7-4 Encryption Algorithm for Key Derivation

Algorithm	Standard	SFR Reference
SHA-256	ISO/IEC 10118-3:2004	FCS_COP.1(c)
HMAC-SHA-256	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”; ISO/IEC 10118	FCS_COP.1(h)
CTR_DRBG (AES)	NIST SP800-90A	FCS_RBG_EXT.1

This encryption key is generated based on a unique value on a per device basis, every time each TOE is powered on, and this encryption key is stored in a volatile memory. Information for encryption key is set only at the start of operation, and is not changed during the operation.

(2) FDP_DSK_EXT.1 Extended: Protection of Data on Disk
FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

When storing data on the HDD, the TOE encrypts the data, using the 256 bits encryption key generated at the time of booting and the AES-XTS encryption algorithm based on ISO/IEC 18033-3, XTS as specified in IEEE 1619, and write into the HDD. When reading out the stored data from the HDD, the TOE decrypts the data, similarly using the 256 bits encryption key generated at the time of booting and the AES-XTS encryption algorithm.
Note that data encryption is provided by the FIPS 140 -2 Certified Cryptographic Module in TOE environment.(CAVP Validation Number : C1933)

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

The random number used in this TOE can collect more than 256bits of entropy by inputting Token to Cryptographic Module.
The random number generation of Cryptographic Module performs processing using CTR_DRBG in accordance with SP800-90A, and includes 1bit of entropy per 1 bit for random number output.
For DRGB random number generation, use the NRGB engine in the Cryptographic Module to set the seed. As the NRBG is configured to generate 1 bit of entropy per 8 'noise' bits and the Conditioning function requires two bits of entropy at its input for each bit of entropy at its output, generating one 256 bits 'full entropy' result requires 256*8*2=4K 'noise' bits. Also, in order to avoid the use of values generated from the same seed, after 256 times 64Kbytes of DRGB random number generation, the automatic generation of random number data by NRGB is executed, and a new value is seeded to the DRGB random number generator by using the random number data.

(4) FCS_CKM.4 Cryptographic Key Destruction
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

The encryption key generated to encrypting HDD is stored in the volatile memory. Therefore, this key is deleted when the TOE is turned off. Also, the key material for generating the encryption key is stored on the main board, but is deleted by performing Data Sanitization function upon TOE disposal.

7.5. Overwrite-Erase Function

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

(1) FDP_RIP.1 Subset residual information protection

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

7.6. Audit Log Function

The audit log function is a function that generates, records and sends to Audit Log server the audit logs when occurring auditable events.

(1) FAU_GEN.1 Audit data generation

The TOE records audit data as listed in Table 7-5, and generates audit logs when auditable events shown in Table 7-5 occur.

Table 7-5 Auditable Events and Audit Data

Auditable Events	Event name	Outcome
Start-up of the audit functions	Power-on[*1]	_
Shutdown of the audit functions	Power-off[*1]	_
Job completion	Completion of print job	Success or Failure
	Completion of scan job	Success or Failure
	Completion of copy job	Success or Failure

	Completion of fax send job	Success or Failure
	Completion of fax receive job	Success or Failure
	Completion of storage / retrieval job	Success or Failure
Unsuccessful User authentication Unsuccessful User identification	Failure of the user identification and authentication	Success or Failure
Use of management functions	Add user	Success or Failure
	Change password	Success or Failure
	Change login user name	Success
	Delete user	Success
	Change security setting	Success
Modification to the group of Users that are part of a role	Modifying user roles	Success
Changes to the time	Changing the Date and Time	Success
Failure to establish session	IPsec Session Establishment Failure	Success or Failure

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

TOE records the following data in audit events:

- Date and time of the event, Type of event, Identification information of the user (Including the identification information of the user who attempted to login), The outcome of the event (success or failure)

(2) FAU_GEN.2 User identity association

For each auditable event, the TOE associates the user identity information that is a cause, with the audit log.

(3) FAU_STG_EXT.1 Extended: External Audit Trail Storage

After the recorded audit log data is temporarily held in the TOE, the log file is transmitted according to the external Audit Log Server set by the U.ADMIN.

The maximum number of audit log data temporarily stored in the TOE is 2300 logs. When the maximum number of recorded audit log data becomes full, the oldest audit log data is deleted and new audit log data can be stored.

(4) FTP_ITC.1 Inter-TSF trusted channel

When the TOE communicates with each type of servers that are trusted IT products,

communication starts between them via a trusted channel. This communication can start from the TOE. The following functions are provided.

- Send to audit log function

The TOE provides trusted channel communications listed below.

Table 7-6 Trusted channel communications provided by the TOE

Destination	Protocols	Encryption algorithm
Audit log Server	IPsec with ESP	3DES(168 bits), AES(128 bits, 192 bits, 256 bits)

(5) FPT_STM.1 Reliable time stamps

The TOE has a system clock inside itself and allows device administrators only to change the time setting of the TOE. The TOE records a date and time of the event with the system clock when auditable events occur. The TOE provides a highly reliable time stamp by recording the time stamps on audit records without delay when the time is recorded by the system clock inside the TOE.

7.7. Security Management Function

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

(1) FMT_MOF.1 Management of security functions behavior

TOE allows device administrators only to change setting the following management functions:

- Auditing
- User Management
- Storage Data Encrypiton
- Firmware update
- Trusted Commnication

(2) FMT_MSA.1 Management of security attributes

The TOE allows device administrators only to use box functions for all boxes as shown below.

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

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

- Read and modify document owner information

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

- Read and modify a box permission

(3) FMT_MTD.1 Management of TSF Data

The TOE provides device administrators only with the operation listed in Table 7-7 on TSF data listed in Table 7-7.

Table 7-7 Operation of TSF Data by Device Administrators

TSF Data	Authorized Operation
Register user information (Login user name, login user password, user authorization, job authorization settings)	Edit, Delete, Newly create
User account lockout policy settings (number of retries until locked, lockout duration)	Modify
Lockout list	Modify
Auto logout time setting	Modify
Password policy settings	Modify
Date and time settings	Modify
Network Encryption Setting	Modify
FAX forward setting	Modify
External Audit Log Server transmitting setting	Modify

The TOE provides normal users with the operation listed in Table 7-8 on TSF data listed in Table 7-8.

Table 7-8 Operaion of TSF Data by Normal Users

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

(4) FMT_SMR.1 Security roles

The TOE maintains the user authorizations of device administrators and normal users, and associates users to the user authorizations.

(5) FMT_SMF.1 Specification of management function

The TOE provides management function of security attributes for box functions as mentioned

in (1), and security management function shown in Table 7-7 and Table 7-8 on TSF data shown in Table 7-7 and Table 7-8.

7.8. Trusted operation

In Trusted operation, a firmware version check function and a function for permitting firmware update are provided to the administrators, and a function for executing the following self-test at the start-up of TOE is provided.

(1) FPT_TUD_EXT.1 Extended: Trusted Update
FCS_COP.1(b) Cryptographic operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

TOE provides administrators with the ability to check firmware versions. The administrator can confirm the firmware version on the device information screen of the operation panel or the web browser.
TOE also provides the ability to allow administrators to update firmware. Firmware updates are only possible when the administrator has successfully authenticated the identity and is logged in. When executing the firmware update, TOE verifies firmware data by using signature verification according to FCS_COP.1(b) and hash calculation according to FCS_COP.1(c) from digital signature attached to firmware data. It conforms to the RSA Digital Signature Algorithm (rDSA) 2048bit, FIPS PUB 186-4, "Digital Signature Standard" for signature verification and uses SHA-256 for the hash algorithm. The firmware update processing is executed only when it is determined that there is no problem as a result of the verification. If the verification of the digital signature fails, the TOE displays an error on the operation panel and aborts the update process.

(2) FPT_TST_EXT.1 Extended: TSF Testing
The TOE performs the following self-test at the TOE start-up.

- Execution the cryptgrachic module selftest
- Check the integrity of executable module of the security function

At the TOE start-up, the TOE performs a self-test of the cryptographic module. In this self-test, a health test of the DRBG and a normal operation test of the encryption function are performed. Also, the TOE also checks the integrity of the executable module of the security function.
In case abnormal operation is found by check at the TOE start-up, the users are notified of this abnormal status by displaying it on the Operation Panel of the TOE. If no abnormal item is found on the Operation Panel, the users assume the TOE correctly operates and so the users

can use the TOE.

7.9. Network Protection Function

The network protection function is a function that encrypts all data in transit over the network between the TOE and trusted IT product and prevents unauthorized alteration and disclosure.

(6) FPT_SKP_EXT.1 Extended: Protection of TSF Data

TOE stores all pre-shared keys, symmetric keys, and private keys used in the network protection function in NAND or volatile memory. NAND and volatile memory are soldered to the main board, are not removable, and do not provide an interface for all users. In addition, data in the volatile memory is erased when the power supply is turned off.

(7) FCS_CKM.1(a) Cryptographic key generation (for asymmetric keys)

TOE generates RSA-based keys in a manner compliance with NIST SP800-56B in generating asymmetric keys for use in network protection functions.

(8) FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)
FCS_COP.1(a) Cryptographic operation (Symmetric encryption/decryption)

TOE encrypts communication using 128bit and 256bit AES-CBC as the encryption algorithm used in the network protection function. To generate 128bit and 256bit target encryption keys, random number generation processing according to FCS_RBG_EXT.1 is performed.

(9) FCS_CKM.4 Cryptographic Key Destruction
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

The TOE stores the session key used by the network protection function in the volatile memory. The data of the volatile memory is erased when the power supply is turned off.

(10) FTP_ITC.1 Inter-TSF trusted channel

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

- Scan to send function
- Box function (Send Function)

The TOE provides trusted channel communications listed below.

Table 7-9 Trusted channel communications provided by the TOE

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

(11) FTP_TRP.1(a) Trusted path (for Administrators)
FTP_TRP.1(b) Trusted path (for Non-administrators)
When the TOE communicates with each type of Client PC that are trusted IT products, communication starts between them via a trusted channel. This communication can start from either of the TOE or the trusted IT product. The following functions are provided.

- Print function
- Operation of a box function from a client PC (web browser)
- Operation of security management function from a client PC (web browser)

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

The TOE provides trusted channel communications listed below.

Table 7-10 Trusted channel communications provided by the TOE

Destination	Protocols	Encryption algorithm
Client PC	IPsec with ESP	3DES(168 bits), AES(128 bits, 192 bits, 256 bits)

(12) FCS_IPSEC_EXT.1 Extended: IPsec selected
FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_COP.1(g) Cryptographic operation (for keyed-hash messege authetication)
FCS_COP.1(b) Cryptographic operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

IPSec with ESP is required for network datagram exchanges with Mail Server/FTP Server/Audit log server and Client PC. IPSec provide confidentiality, integrity and authentication of the endpoints. Supported encryption options for is AES. SHA-2 is supported for MACs.
ISAKMP and IKEv1 are used to establish the Security Association (SA) and keys for the IPSec exchanges. Diffie-Hellman is used for IKEv1 Key Derivation Function as specified in RFC2409, using Oakley Groups 14. In the ISAKMP exchange, a pre-shared keys is configured by administrators and validated between endpoints.
The key size specified in the SA exchange is 128 or 256 bits and the encryption algorithm is

AES-CBC and the Hash Authentication Algorithm may be SHA-1, SHA-256 (as configured by administrators).
Keys generated for the IKEv1 exchanges are performed per RFC2409. If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded. All keys are held in memory and is only valid with the corresponding SA. Once the SA is terminated the key cannot be used.
The TOE can be configured as IPsec security policy database(SPD) to accept or not(Allowed or Denied) communications from networks other than those specified in the IPsec policy. Allowed is set, communication from networks other than those specified in the IPsec rule settings is also accepted. Denied is set, the packet is discarded without accepting communications from networks other than those specified in the IPsec rule settings.
Note that random number generation based on FCS_RBG_EXT.1 in key generation is provided by FIPS 140-2 certified cryptographic modules in TOE environment.（CAVP Validation Number : C1892）

The IPsec protocol used by TOE is as follows. Note that device administrators can select an item having multiple selections, and only the administrator can set or change this selection.

- Encapsulation Settings: Transport mode
- Security Protocol: ESP
  - Cryptographic algorithms: AES-CBC-128, AES-CBC-256
  - Authentication algorithms: HMAC-SHA-1, HMAC-SHA-256
- Key exchange: IKEv1
  - IKEv1 algorithms: AES-CBC-128, AES-CBC-256
  - IKEv1 mode: Main Mode
  - IKEv1 SA lifetimes(phase1): 1,800 – 86,400 seconds
  - IKEv1 SA lifetimes(phase2): 1,800 – 86,400 seconds
  - Diffie-Hellman Group: DH Group 14
- Peer Authentication: RSA, Pre-shared Keys
- Authentication method: Pre-shared Keys
  - Pre-shared Keys: 1-128 length and ASCII charactoers
  - Authentication algorithms: SHA-1, SHA-256

7.10. PSTN Fax-Network Separation

TOE ensure separation between the PSTN fax line and the Internal Network.

(1) FDP_FXS_EXT.1 Extended: Fax separation
The TOE has a fax modem function, but provides only fax transmission and fax reception functions over the PSTN.

Since only the ITU-T G3 protocol is supported as a fax interface, only transmission and reception using the fax protocol are accepted. Since a data modem function is not provided, data communication commands from the outside are not accepted. Thus, the TOE cannot be illegally accessed from the PSTN, and the TOE cannot be bridge-connected to the internal network.

7.11. Deviations From Allowed Cryptographic Standards

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

1. Hashing: SHA-1 is supported for backward compatibility with remote systems.
2. Block cipher: AES-XTS is supported for storage encryption.

8. Acronyms and Terminology

8.1. Definition of terms

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

Table 8-1 Definitions of terms used in this ST

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

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

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

8.2. Definition of acronyms

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

Table 8-2 Definitions of acronyms used in this ST

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

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

(The final page)