KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 With UK-112 Security Target

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

Version 1.17

2021/04/02

Konica Minolta Co., Ltd.

<Update History>

Date	Ver	Department in charge	Approver	Confirmed by	Author	Updated contents
2020/11/04	1.00	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	First edition
2020/11/20	1.01	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2020/11/27	1.02	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2020/12/08	1.03	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2020/12/22	1.04	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2020/12/24	1.05	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/01/06	1.06	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/01/18	1.07	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/01/25	1.08	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/02/02	1.09	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/02/04	1.10	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/02/08	1.11	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/02/10	1.12	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/02/17	1.13	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/02/26	1.14	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/03/08	1.15	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/03/18	1.16	PP Service Development Dept. 1	Haga	Yoshino	Yasukaga	Correction of errors
2021/04/02	1.17	PP system control development department	Haga	Yoshino	Yasukaga	Correction of errors

Table of Contents

1. ST introduction 6
1.1. ST reference 6
1.2. TOE reference 6
1.3. TOE overview 6
1.3.1. *Type of TOE 6*
1.3.2. *Usage and key security features 6*
1.3.3. *Operating environment 7*
1.3.4. *Non-TOE hardware/software required for TOE 8*
1.4. TOE description 8
1.4.1. *Physical scope of the TOE 8*
1.4.2. *Logical scope of the TOE 10*
1.5. Term 12
2. Conformance claims 15
2.1. CC Conformance claims 15
2.2. PP claim 15
2.3. PP Conformance rationale 15
3. Security Problem Definition 16
3.1. Users 16
3.2. Assets 16
3.2.1. *User Data 16*
3.2.2. *TSF Data 16*
3.3. Threats 17
3.4. Organizational Security Policies 17
3.5. Assumptions 17
4. Security Objectives 19
4.1. Security Objectives for the Operational environment 19
5. Extended components definition 20
5.1. FAU_STG_EXT Extended: External Audit Trail Storage 20
5.2. FCS_CKM_EXT Extended: Cryptographic Key Management 20
5.3. FCS_IPSEC_EXT Extended: IPsec selected 21
5.4. FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining) 23
5.5. FCS_KDF_EXT Extended: Cryptographic Key Derivation 24
5.6. FCS_PCC_EXT Extended: Cryptographic Password Construction and Conditioning 25
5.7. FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation) 25
5.8. FCS_SNI_EXT Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation 26
5.9. FDP_DSK_EXT Extended: Protection of Data on Disk 27
5.10. FIA_PMG_EXT Extended: Password Management 28
5.11. FIA_PSK_EXT Extended: Pre-Shared Key Composition 29
5.12. FPT_KYP_EXT Extended: Protection of Key and Key Material 30
5.13. FPT_SKP_EXT Extended: Protection of TSF Data 31
5.14. FPT_TST_EXT Extended: TSF testing 31
5.15. FPT_TUD_EXT Extended: Trusted Update 32
6. Security Requirements 34
6.1. Security functional requirements 34
6.1.1. *Class FAU: Security audit 34*
6.1.2. *Class FCS: Cryptographic support 35*

6.1.3. *Class FDP: User data protection* *39*
6.1.4. *Class FIA: Identification and authentication* *41*
6.1.5. *Class FMT: Security management* *44*
6.1.6. *Class FPT: Protection of the TSF* *47*
6.1.7. *Class FTA: TOE access* *47*
6.1.8. *Class FTP: Trusted path/channels* *48*
6.1.9. *Class FPT: Protection of the TSF* *49*
6.1.10. *Class FCS: Cryptographic support* *49*
6.1.11. *Class FDP: User data protection* *50*
6.1.12. *Class FCS: Cryptographic support* *50*
6.1.13. *Class FCS: Cryptographic support* *51*
6.1.14. *Class FCS: Cryptographic support* *53*
6.1.15. *Class FIA: Identification and authentication* *53*
6.1.16. *Class FCS: Cryptographic support* *54*
6.1.17. *Class FCS: Cryptographic support* *54*
6.2. Security assurance requirements 56
6.3. Security requirements rationale 57
6.3.1. *The dependencies of security requirements* *57*
7. TOE Summary specification 60
7.1. Identification and authentication function 60
7.2. Access control function 62
7.3. Storage encryption function 63
7.4. Trusted communications function 67
7.5. Security management function 70
7.6. Audit function 71
7.7. Software update verification function 73
7.8. Self-testing function 73

Table of figures

Figure 1-1 Use of TOE 7
Figure 1-2 Physical scope of TOE 8
Figure 1-3 Logical scope of TOE 11

Table of Contents

Table 1-1 Evaluated Configuration 8
Table 1-2 configuration 9
Table 1-3 TOE firmware configuration 9
Table 1-4 Guidance List 10
Table 1-5 Components of TOE 10
Table 1-6 Basic functions of TOE 11
Table 1-7 Security function of TOE 12
Table 1-8 Terms 13
Table 3-1 User Categories 16
Table 3-2 Asset categories 16
Table 3-3 User Data Type 16
Table 3-4 TSF Data 16
Table 3-5 Threats for the TOE 17

Table 3-6 Organizational Security Policies for the TOE ... 17
Table 3-7 Assumptions for the TOE ... 18
Table 4-1 Security Objectives for the Operational environment ... 19
Table 6-1 Audit data requirements ... 34
Table 6-2 D.USER.DOC Access Control SFP ... 40
Table 6-3 D.USER.JOB Access Control SFP ... 41
Table 6-4 Authentication failure handling ... 42
Table 6-5 Management of Security Functions behavior ... 44
Table 6-6 Management of Object Security Attribute ... 45
Table 6-7 Operation of TSF Data (1) ... 45
Table 6-8 Operation of TSF Data (2) ... 45
Table 6-9 Operation of TSF Data (3) ... 46
Table 6-10 list of management functions ... 46
Table 6-11 TOE Security Assurance Requirements ... 56
Table 6-12 The dependencies of security requirements ... 57
Table 7-1 List of Security Functions ... 60
Table 7-2 Special Characters Available for Passwords ... 61
Table 7-3 Cryptographic algorithm ... 63
Table 7-4 Encryption Key for Storage Encryption ... 63
Table 7-5 Special characters (32 characters) that can be used for the password ... 64
Table 7-6 Data to be encrypted for each device (portable storage medium) ... 65
Table 7-7 Data to be encrypted for each device (other than portable storage media) ... 65
Table 7-8 Storage and destruction of keys ... 67
Table 7-9 Reliable path (FTP_TRP.1(a)) available to the administrator ... 68
Table 7-10 Encrypted communication provided by TOE ... 68
Table 7-11 Destination and Destination of Key ... 70
Table 7-12 Administrative functions provided to U.ADMIN ... 70
Table 7-13 Administrative functions provided to U.NORMAL ... 71
Table 7-14 List of Audited Events ... 71
Table 7-15 Audit Log Information Specifications ... 72

1. ST introduction

1.1. ST reference

- ST name	:	KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 with UK-112 Security Target
- ST version	:	1.17
- Creation date	:	April 02, 2021
- Author	:	Konica Minolta Co., Ltd.

1.2. TOE reference

- TOE name	:	KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 with UK-112
- Version	:	GM2-20

The TOE above consists of the main unit (KONICA MINOLTA Accurio Press C4080, KONICA MINOLTA Accurio Press C4070, KONICA MINOLTA Accurio Print C4065, or firmware version GM2-20) and the mandatory HDD unit (product name: UK-112). The TOE version GM2-20 consists of a combination of the firmware type and version name described in Table 1-3, which is information for identifying firmware. KONICA MINOLTA Accurio Print C4065 is not sold in Japan (KONICA MINOLTA Accurio Press C4080/Accurio Press C4070 can be purchased in Japan and overseas).

1.3. TOE overview

This TOE is a digital multifunction device (hereinafter referred to as MFP) used in a commercial information processing environment where medium document security, network security, and information assurance are basically required. This environment typically handles confidential and non-confidential information that is handled in day-to-day business operations.

1.3.1. Type of TOE

TOE is an MFP used in the network environment (LAN) and has a function for copy, scan, and store and retrieve documents. This TOE does not have a fax function or a function to print and store print jobs from a PC.

1.3.2. Usage and key security features

The TOE is connected to a LAN and has functions that allow users to scan, copy, and store and retrieve documents. In addition, the following security features are provided to protect user documents and security-related data: Identification and authentication function that identifies users and allows only authorized users to use the TOE. Access control function that restricts access to documents and various TOE operations according to the authority given to the user. Security management function that restricts security function settings to users with administrator privileges. Audit function that records security-related events and sends them to a log server. Trusted communications function that protects the communication between the TOE and external IT devices by IPsec. Storage encryption function that encrypts the data recorded on HDD / SSD. Software update verification function that prevents updates due to unauthorized firmware. Self-testing function that demonstrates the normal operation of TSF.

1.3.3. Operating environment

Figure 1-1 shows the TOE operation environment. TOE is connected to the LAN. The user can operate the TOE by communicating via the TOE's operation panel or LAN.

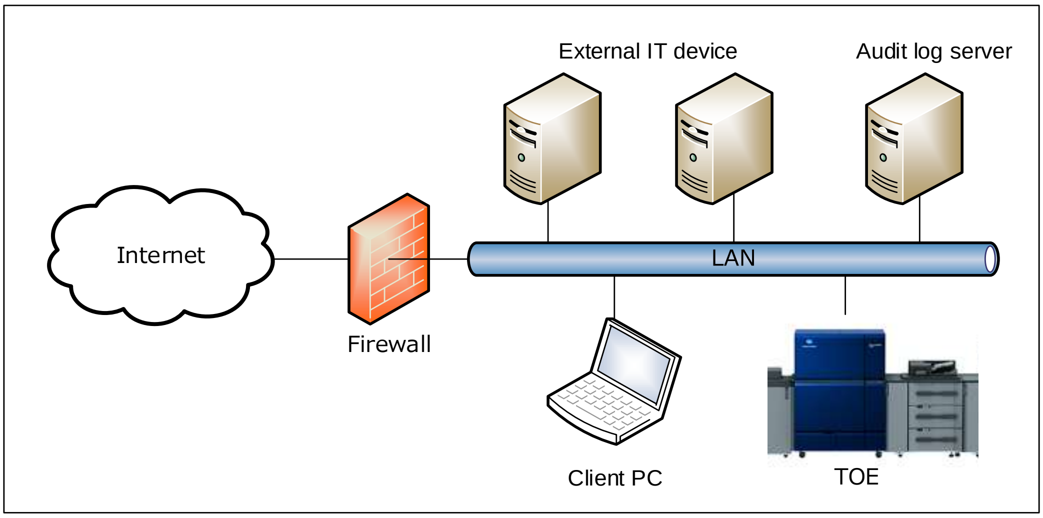


Figure 1-1 Use of TOE

(1) TOE (MFP body)

TOE is connected to the office LAN. The user can perform the following processing from the operation panel.

- Various settings of TOE
- Copy of paper documents, storage as electronic documents, and network transmission
- Printing and deleting stored documents

(2) LAN

The network used in the TOE installation environment.

(3) Firewall

Device to prevent network attacks from the Internet to the in-office LAN.

(4) Client PC

The web browser software can be used to access TOE from the client PC and perform the following operations.

- Web Connection (after administrator authentication, TOE's firmware version can be viewed on the browser)

(5) Audit log server

The server to which the TOE audit function is to be sent. The user can specify the syslog server as the destination for audit log information.

(6) External IT device (to which electronic documents are sent)

An external IT device to which electronic documents are sent. The user can specify a WebDAV server, an SMB server, or an FTP server as the destination.

1.3.4. Non-TOE hardware/software required for TOE

The configuration used to evaluate TOE as the hardware/software required for using TOE is shown below.

Table 1-1 Evaluated Configuration

Hardware/software		Versions used in the evaluation
Client PC (OS)		Windows 10 Pro
	Web browser	Microsoft Internet Explorer 11
	IPsec	Built-in operating system
Audit log server		Rsyslog 8.1901.0
	IPsec	Strongswan 5.8.0
FTP server		Vsftpd 3.0.3
	IPsec	Strongswan 5.8.0
WebDAV server		Apache2 2.4.38
	IPsec	Strongswan 5.8.0
SMB server		Samba 4.9.5
	IPsec	Strongswan 5.8.0

1.4. TOE description

This chapter outlines the physical and logical scope of the TOE.

1.4.1. Physical scope of the TOE

1.4.1.1. Physical configuration of TOE

As shown in the figure below, the TOE physical scope is an MFP consisting of an operation panel, scanner unit, printer unit, control board, HDD/SSD, USB I/F, and Network I/F.

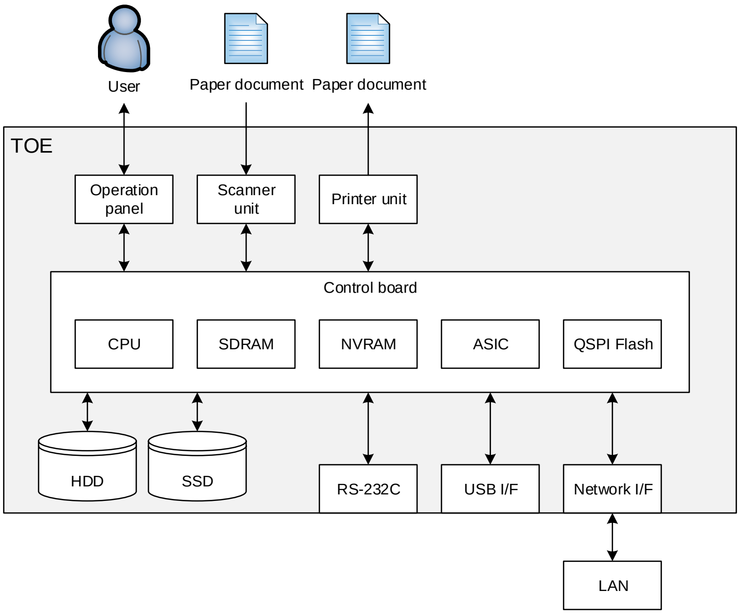


Figure 1-2 Physical scope of TOE

Table 1-2 configuration

No.	Function	Definition
1	Operation panel	A device for operating TOE with a touch panel liquid crystal display and hardware keys such as start and stop keys.
2	Scanner unit	A device for reading figures and pictures from paper and converting them into electronic data.
3	Printer unit	A device for printing and outputting image data converted for printing by instructions from a control board.
4	Control board	A device that controls TOE.
5	CPU	Central processing unit
6	RAM	Volatile memory used as a working area.
7	ASIC	Integrated circuit for specific use that incorporates the compression deployment function of image data.
8	NVRAM	A non-volatile memory in which setting data or TSF data that determines the operation of the TOE are stored.
9	QSPI Flash	Semiconductor storage that stores the key material of the encryption key (KEK). It is not a portable storage medium. The device is mounted directly on a substrate and cannot be detached.
10	HDD- SSD	It is used as a removable storage medium for storing image data, temporary image data, and work area.
11	RS-232C I/F	An interface that can be serially connected. It can be used for the remote diagnostic function (CS Remote Care) by connecting to a modem connected to a public line, but its use is prohibited in TOE.
12	Network I/F	An interface that supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet.
13	USB I/F	A USB interface that connects operation devices such as a keyboard and a mouse and USB memory and rewrites firmware and stores and retrieves image data. However, the use of USB devices is prohibited in TOE (excluding the use of USB memory in the firmware update function).

1.4.1.2. TOE's firmware configuration

The TOE firmware components are as follows.

Table 1-3 TOE firmware configuration

Type of firmware	ROM type	Definition	Version name (GM2-20 configuration FW)
Image control system/1	I1	Image Control Processing and Operation Part Control	AC570Y0-00I1-GM2-20
Image control system/2	I2	As above	AC570Y0-00I2-G00-20
Image control system/3	I3	As above	AC570Y0-00I3-G00-20
Image control system/4	I4	As above	AC570Y0-00I4-GM2-20
Image control system/5	I5	As above	AC570Y0-00I5-GM2-20
ADF system	F	Automatic document feeder control	AAMP0Y0-00F1-G00-03
Sound source system	T	Audio data of the control unit	AC570Y0-00T1-G00-10
Browser feature	W	Browser processing	AC570Y0-00W1-G00-20
Scanner	L	Scanner substrate processing	AC570Y0-00L1-G00-10
Printer system	C	Print control	AC570Y0-00C1-G00-20

Network control	P9	Network control processing	AC570Y0-00P9-GM2-20
Printer sub-CPU	D	PCB control	AC570Y0-00D1-G00-1000

1.4.1.3. Guidance

The following is a list of guidance. Guidance for general users (User's Guide) is provided by the dealer to the user in the form of html file by contacting the URL to which the manual should be referred. In addition, guidance on security functions (User's Guide Security Function) is provided by the dealer to the user using portable storage media in the format of an exe file.

Table 1-4 Guidance List

Name	Ver.	Supplement
KONICA MINOLTA Accurio Press C4080/C4070 User's Guide	02.10.00	Japanese version
KONICA MINOLTA Accurio Press C4080/Accurio Press C4070 User's Guide Security Functions (Administrator)	1.0 (2021-04-02)	Japanese version
KONICA MINOLTA Accurio Press C4080/Accurio Press C4070 User's Guide Security Functions (Users)	1.0 (2021-04-02)	Japanese version
KONICA MINOLTA AccurioPress C4080/C4070 / AccurioPrint C4065 User's Guide	02.10.00	English version
KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 User's Guide Security Functions (Administrator)	1.0 (2021-04-02)	English version
KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 User's Guide Security Functions (User)	1.0 (2021-04-02)	English version

The Japanese version of the guidance will be distributed only in Japan, and the English version will be distributed only overseas (outside Japan). KONICA MINOLTA Accurio Print C4065 will not be sold in Japan (KONICA MINOLTA Accurio Press C4080/Accurio Press C4070 can be purchased in Japan and overseas).

1.4.1.4. Identification of the TOE components

The components of the TOE are as follows.

Identification of the MFP body and HDD unit constituting the TOE is as follows.

The MFP main unit is in a format that incorporates the hardware and firmware constituting the TOE, and is provided to the user by the dealer with a technician who performs the initialization. In addition, the HDD unit is transported in the form of optional equipment.

Table 1-5 Components of TOE

Component	Identification	FW version
MFP main unit (Any one of the right)	KONICA MINOLTA AccurioPress C4080, KONICA MINOLTA AccurioPress C4070, KONICA MINOLTA AccurioPrint C4065	FW version GM2-20
HDD unit	UK-112	

1.4.2. Logical scope of the TOE

The security functions and basic functions of TOE are described below.

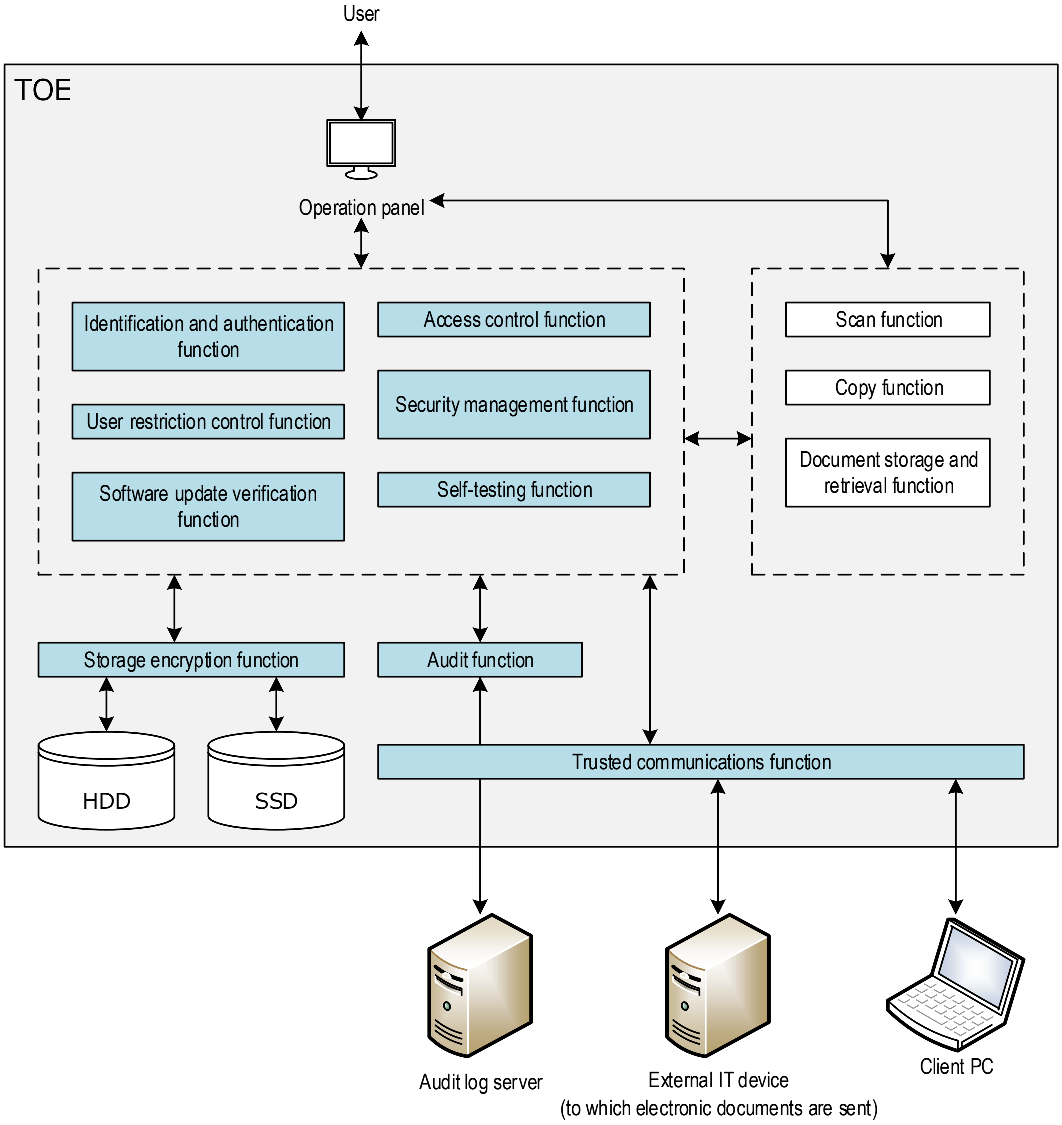

User
TOE
Operation panel
Identification and authentication function
Access control function
User restriction control function
Security management function
Software update verification function
Self-testing function
Scan function
Copy function
Document storage and retrieval function
Storage encryption function
Audit function
HDD
SSD
Trusted communications function
Audit log server
External IT device
(to which electronic documents are sent)
Client PC

Figure 1-3 Logical scope of TOE

1.4.2.1. Basic functions

TOE has the following basic functions.

Table 1-6 Basic functions of TOE

No.	Function	Definition
1	Scan function	Ability to read paper documents, generate electronic documents, and send them to external IT devices (WebDAV servers, SMB servers, FTP servers) by manipulating the user's operation panel
2	Copy function	A function that reads a paper document, generates an electronic document, and prints a copy of the document or saves it in the HDD by the user's operation from the operation panel.
3	Document storage and retrieval function	This is a function to read paper documents, generate electronic documents, store them on an HDD, or extract stored electronic documents from an HDD and print them. Stored electronic documents can be modified or deleted.

1.4.2.2. Security function

The security functions of TOE are described below.

Table 1-7 Security function of TOE

No.	Function	Definition
1	Identification and authentication function	A function to verify that a person who intends to use the TOE is an authorized user using identification and authentication information obtained from the user, and to permit the use of the TOE only to a person who is determined to be an authorized user. Only the main unit authentication method in which TOE itself performs identification and authentication can be used for the authentication method. This function includes the following functions. - Function to stop authentication for a certain period of time when authentication fails - Function to display the entered password in dummy characters at login - Ability to register only the password that meets the minimum password length conditions set by the administrator to protect password quality - Function to terminate the session at the operation panel if there is no operation for a certain period of time by the user who has been identified and authenticated.
2	Access control function	A function that restricts access to protected assets in the TOE so that only authorized users can access them.
3	Storage encryption function	Function to encrypt data stored on HDDs and SSDs to protect them from leakage.
4	Trusted communications function	A function to prevent information leakage due to wiretapping on a network when using a LAN. Communication data between the client PC and the TOE and communication data between the audit log server and external IT devices (servers that can be used as a destination for sending electronic documents; WebDAV server, SMB server, and FTP server) and the TOE is encrypted by IPsec communication.
5	Security management function	A function that controls the operation of TSF data and controls the behavior of security functions on the basis of the privileges given to the user's role or the privileges given to each user to authorized users of TOE that are authenticated by the identification and authentication function. These include settings for security enhancement, user creation/password changes, audit log server settings, and date and time changes.
6	Audit function	A function to send logs of events related to TOE use and security (hereinafter referred to as audit events) to an external audit log server together with date and time information.
7	Software update verification function	Function to perform Digital Signature Verification to ensure the authenticity of firmware before executing firmware updates for TOE
8	Self-testing function	This is a function to verify that the TSF execution firmware is normal when the TOE starts.

1.5. Term

The following abbreviations and terms are used in this ST.

Table 1-8 Terms

Designation	Definition
Electronic document	Electronic documents are electronic data that convert information such as images, letters, and graphics into electronic data.
Paper documents	Paper documents are paper documents that contain information such as images, letters, and graphics.
Operation panel	The operation panel is the name of the touch panel display and operation button attached to the KONICA MINOLTA AccurioPress C4080/AccurioPress C4070/AccurioPrint C4065 series enclosure.
SMB	An SMB is an application protocol that enables computers to communicate with each other on a network in a Microsoft operating system.
User	A general user whose user name and login password are registered in TOE by the administrator. User ID is associated with successful login identification and authentication function.
Administrator	Users who know the administrator password. Associated with Admin ID by successful identification and authentication function required when administrator function is used.
Service mode	Setup screens for service engineers (hereinafter referred to as CE) who are engineers to install, maintain, and repair TOE. Functions such as fine tuning of a device such as a storage medium or a scanner print can be performed. The service mode can be checked and changed only from the operation panel. However, this function can be disabled by setting the service login permission setting function (administrator can configure this function).
SC code	Error codes displayed on the operation panel when a significant software or hardware error occurs. When the SC code is displayed, the TOE stops the operation and moves to the state where the operation is not accepted. When this code appears, the administrator is guided to call the service engineer.
Network Management Functions	This is a function that can be used after an administrator's identification and authentication via the network (remote management function). It includes the Internet ISW function (function to rewrite TOE from an external server using the Internet) and Web Connection (function to change the setting of TOE and check the status using the web browser). When the security enhancement setting is enabled, only the firmware version check function of the Web Connection is available, and other functions are not available.
FTP transmission	Function to upload electronic documents to an FTP server.
SMB transmission	The ability to send electronic documents to shared folders on computers and servers.
WebDAV transmission	The ability to upload electronic documents to a WebDAV server.
Auto reset	This function automatically logs out when there is no access at the predetermined auto reset time during login.
Autoreset time	When this time has elapsed, the system automatically logs out. The operation from the operation panel is targeted.
Job	Document processing tasks sent to the hardcopy device. A single processing task can process more than one document.
Security enhancement settings	This is a function to set the settings related to the behavior of the security function in a secure value and to maintain those settings. By enabling this function, the use of TOE update function via the network, network setting function with low security level, etc. is prohibited, or a warning screen is displayed when using this function. In addition, a warning screen is displayed when changing the set value, and when changing the set value (only the administrator can execute it), the security enhancement setting is disabled. The

Designation	Definition
	TOE environment is only enabled when the security enhancement setting is enabled.
User ID	Identifier assigned to the general user. The TOE identifies the user by its identifier.
Admin ID	Identifier assigned to the administrator. The TOE identifies the user by its identifier.
User management	This function registers, changes, and deletes users.
Authenticating user identities	Function to authenticate TOE users. There are three types of authentication: main unit authentication, intermediate authentication, and external authentication. Only main unit authentication can be used when the security enhancement setting is valid.
Login	Execute identification and authentication in TOE using the username and login password.
Encryption password	Data used in the generation of encryption keys used in the encryption of HDDs and SSDs. TOE generates the encryption key using the string set in the encryption password.
Audit function	This function generates and records an audit log for the event to be audited and sends the log to the log server.
Trusted communications function	A function to encrypt and protect data to be exchanged via a LAN.
Firmware	This software has the function of basic control of TOE and its peripheral equipment (finisher), and TOE consists of multiple firmware. This control firmware and controller firmware are used to realize the TSF function.
Firmware update	A function to update firmware using update data obtained through a network or USB memory. Only updates using USB memory can be performed when the security enhancement setting is enabled. Also called ISW.

2. Conformance claims

2.1. CC Conformance claims

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

CC version	:	Version 3.1 Release 5
CC conformance	:	Part2 (CCMB-2017-04-002) Extended, And Part3 (CCMB-2017-04-003) Conformant

2.2. PP claim

This ST conforms to the following PP.

PP identification	:	
PP Title	:	Protection Profile for Hardcopy Devices
PP registration	:	
PP version	:	1.0 dated September 10, 2015
Date	:	September 10, 2015
Errata	:	Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

2.3. PP Conformance rationale

The following conditions requested by PP are met and "Exact Conformance" is as requested 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
  None

3. Security Problem Definition

This chapter describes the definition, assumptions, threats, and organisational security policies of users and properties to be protected.

3.1. Users

TOE users are classified as follows.

Table 3-1 User Categories

Designation	Asset category	Definition
U.NORMAL	Normal User	A User who has been identified and authenticated and does not have an administrative role
U.ADMIN	Administrator	A User who has been identified and authenticated and has an administrative role

3.2. Assets

Protected assets are User Data, TSF Data. Each asset is defined as follows:

Table 3-2 Asset categories

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

3.2.1. User Data

User Data consists of the following two types.

Table 3-3 User Data Type

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 consists of the following two types:

Table 3-4 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

3.3. Threats

This section describes threats to assets described in clause in 3.2.

Table 3-5 Threats for the TOE

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate while in a degraded state.
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

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

Table 3-6 Organizational Security Policies for the TOE

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	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.

3.5. Assumptions

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

Table 3-7 Assumptions for the TOE

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

4. Security Objectives

4.1. Security Objectives for the Operational environment

This section describes the Security Objectives that must be fulfilled in the operational environment of the TOE.

Table 4-1 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.
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.

5. Extended components definition

This chapter defines the extended security functional requirements. All extension requirements are defined in HCD-PP.

5.1. FAU_STG_EXT Extended: External Audit Trail Storage

Family Behavior:
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.

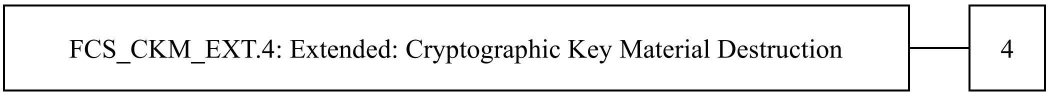
Rationale:
The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided 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 Behavior:
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 Behavior:
This family addresses requirements for protecting communications using IPsec.

Component leveling:

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_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric Encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature Generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit

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, 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]].

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_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family Behavior:
This family provides the specification to be used for using multiple layers of encryption keys to ultimately secure the protected data encrypted on the storage.

Component leveling:

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(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].

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.

5.5. FCS_KDF_EXT Extended: Cryptographic Key Derivation

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

Component leveling:

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	***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.		

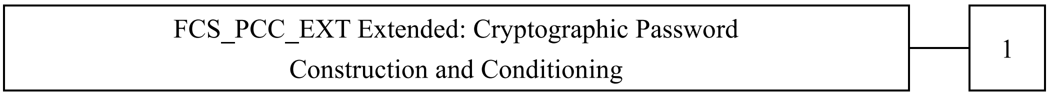
Rationale:
The TSF is required to specify the means by which an intermediate key is derived from a specified set of submasks using the specified hash functions.
This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key

chains, and it is therefore placed in the FCS class with a single component.

5.6. FCS_PCC_EXT Extended: Cryptographic Password Construction and Conditioning

Family Behavior:
This family ensures that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.

Component leveling:


FCS_PCC_EXT Extended: Cryptographic Password Construction and Conditioning
1

FCS_PCC_EXT.1 Cryptographic Password Construction and Conditioning, requires the TSF to accept passwords of a certain composition and condition them appropriately.

Management:
No specific management functions are identified

Audit:
There are no auditable events foreseen.

FCS_PCC_EXT.1 ***Extended: Cryptographic Password Construct and Conditioning***

Hierarchical to : No other components

Dependencies : FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)

FCS_PCC_EXT.1.1 A password used to generate a password authorization factor shall enable up to [assignment: positive integer of 64 or more] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: other supported special characters]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [HMAC-[selection: SHA-256, SHA-384, SHA-512]], with [assignment: positive integer of 1000 or more] iterations, and output cryptographic key sizes [selection: 128, 256] that meet the following: [assignment:PBKDF recommendation or specification].

Rationale:
The TSF is required to ensure that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.
This extended component protects the Data Encryption Keys using cryptographic algorithms and Robust BEV in the maintained key chains, and it is therefore placed in the FCS class with a single component.

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

Family Behavior:
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: Cryptographic Operation (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 at least one 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.

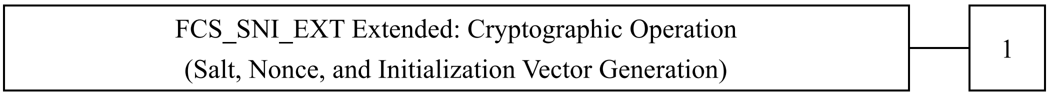
Rationale:
Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.

This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.8. FCS_SNI_EXT Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation

Family Behavior:
This family ensures that salts, nonces, and IVs are well formed.

Component leveling:


FCS_SNI_EXT Extended: Cryptographic Operation
(Salt, Nonce, and Initialization Vector Generation)
1

FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation), requires the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE to be performed in the specified manner.

Management:
No specific management functions are identified

Audit:
There are no auditable events foreseen.

FCS_SNI_EXT.1 ***Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)***

Hierarchical to : No other components

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

FCS_SNI_EXT.1.1 The TSF shall only use salts that are generated by a RNG as specified in FCS_RBG_EXT.1.

FCS_SNI_EXT.1.2 The TSF shall only use unique nonces with a minimum size of [64] bits.

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner: [
- CBC: IVs shall be non-repeating,
- CCM: Nonce shall be non-repeating.
- XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer,
- GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.
].

Rationale:
The TSF is required to ensure that the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE to be performed in the specified manner.
This extended component protects the communication data and storage data using cryptographic algorithms with specified Salt, Nonce and Initialization Vector Generation, and it is therefore placed in the FCS class with a single component.

5.9. FDP_DSK_EXT Extended: Protection of Data on Disk

Family Behavior:
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, 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.

5.10. FIA_PMG_EXT Extended: Password Management

Family Behavior:
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 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.

5.11. FIA_PSK_EXT Extended: Pre-Shared Key Composition

Family Behavior:

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.1.3 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].

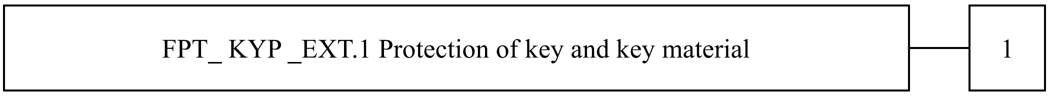
Rationale:
Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

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

5.12. FPT_KYP_EXT Extended: Protection of Key and Key Material

Family Behavior:
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.

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.

5.13. FPT_SKP_EXT Extended: Protection of TSF Data

Family Behavior:
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 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.		

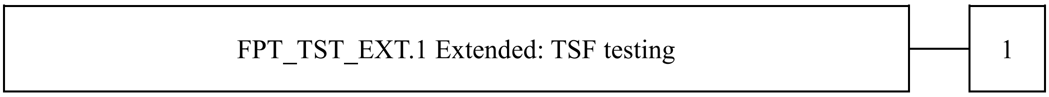
Rationale:
Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.

This extended component protects the TOE by means of strong authentication using Preshared Key, and it is therefore placed in the FPT class with a single component.

5.14. FPT_TST_EXT Extended: TSF testing

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

Component leveling:



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.

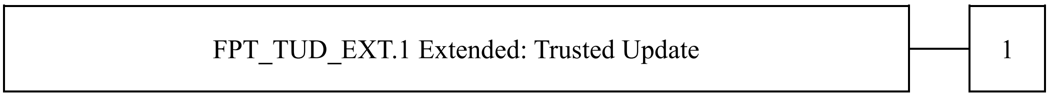
Rationale:
TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing.In particular, there is no SFR defined for TSF testing.

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

5.15. FPT_TUD_EXT Extended: Trusted Update

Family Behavior:
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 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 **Extended: Trusted Update**

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.

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 chapter describes the security requirements.

6.1. Security functional requirements

This section describes the security function requirements of TOE to implement the security policy specified in Section 4.1. The security function requirements are quoted from the security function requirements specified in CC Part 2. For security functional requirements not specified in CC Part 2, see Section 5.

<How to specify security function requirements "operation">

Decorations are made based on the following rules in the description of the Functional Elements below.

- **The notation given in bold indicates** the part of the SFR that has been completed or elaborated in the PP and relates to the original SFR or Extended Component definition in Common Criteria Part 2.
- *Italic fonts* indicate the text in the SFR selected or assigned in this ST. The selected or assigned values are shown in blue.
- ***Balldeutaric font*** indicates the text in the SFR selected and/or completed in ST for the portion of the SFR that is completed or detailed in PP. The selected or assigned values are shown in blue.
- **The underscore** shows the results of this ST detail (in the case of tables, only the title is specified).
- SFR components in parentheses followed by characters, e.g., (a), (b),..., indicate repeats.
- Extended components are identified by adding "_EXT" to the SFR identification.

Mandatory SFR

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 Audit data requirements

Auditable event	Relevant SFR	Additional	Details

		Information	
Job completion	FDP_ACF.1	Type of job	- Completion of copying - Completion of scanning - Saving a copy job - Read out a saved job - Print the saved job - File output of saved jobs - Deleting a saved job - Duplicating a saved job - Modifying a saved job
Unsuccessful User authentication	FIA_UAU.1	None	Successful login Login failures
Unsuccessful User identification	FIA_UID.1	None	Successful login Login failures
Use of management functions	FMT_SMF.1	None	- Using Security Management Functions
Modification to the group of Users that are part of a role	FMT_SMR.1	None	Do not record because user role change function does not exist.
Changes to the time	FPT_STM.1	None	- Change in the time
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a)	Reason for failure	- Reasons for Failure to Establish Communication

FAU_GEN.2 **User identity association**

(for O.AUDIT)

Hierarchical to : No other components

Dependencies : FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

FAU_STG_EXT.1 **Extended: External Audit Trail Storage**

(for O.AUDIT)

Hierarchical to : No other components

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

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

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_COP.1(i) Cryptographic operation (Key Transport)]
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 field-based key establishment schemes;***
- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based 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 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes
- 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(a) Cryptographic Operation (Symmetric Encryption/decryption)
FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_CKM.1.1(b)
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
- 256 bit

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 SP800-38A

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

[assignment: ***2048 bits or greater*****]**

- 2048bits

[**selection:** Case: Digital ...]

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

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

(for O.STORAGE_ENCRYPTION and O.COMMS_PROTECTION)

Hierarchical to : No other components.

Dependencies : No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [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 at least one 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)]

- [assignment: *number of software-based sources*] software-based noise source(s)

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

- one

[selection: *128 bits, 256 bits*]

- 256 bits

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 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

Refinement [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 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

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

[assignment: *rules **that 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"**
Scan	**Operation:**	***Submit a document for scanning***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2)	Denied	Denied	Denied
	U.ADMIN	Denied	Denied	Denied	Denied
	U.NORMAL		Denied	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Copy	**Operation:**	***Submit a document for copying***	***View scanned image or Release printed copy output***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2)	Denied	Denied	
	U.ADMIN	Denied	Denied	Denied	Denied
	U.NORMAL		Denied	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Storage / retrieval	**Operation:**	***Store document***	***Retrieve stored document***	***Modify stored document***	***Delete stored document***
	Job owner	(note 1)			
	U.ADMIN	Denied		Denied	
	U.NORMAL		Denied	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied

[Supplement] Table 6-2 describes the SFP in the following situations.

- **Scan :** SFP for image data temporarily held in the HCD when the user performs the operation of sending scanned image data to the scanned image destination.
- **Copy :** SFP for image data temporarily held in the HCD when the user performs the operation of printing the scanned image data.
- **Storage / retrieval :**
  SFP for image data stored on an HDD when the user saves the scanned image data to an HDD.

※Since this TOE does not incorporate the fax function, there is no operation and access control when "Fax send" or "Fax receive" is used. Also, since the print function from the network is not provided, there is no operation and access control in "Print".

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

		"Create"	"Read"	"Modify"	"Delete"
Scan	**Operation:**	***Create scan job***	***View scan status / log***	***Modify scan job***	***Cancel scan job***
	Job owner	(note 2)		Denied	Denied
	U.ADMIN	Denied		Denied	Denied
	U.NORMAL			Denied	Denied
	Unauthenticated	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	Denied
	U.NORMAL			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		Denied	
	U.NORMAL		Denied	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied

[Supplement] Table 6-3 describes the SFP in the following situations.

- **Scan :** SFP for job data of jobs temporarily saved in HCD when the user performs the operation of sending scanned image data to the scanned image destination.
- **Copy :** SFP for job data of jobs temporarily saved in HCD when the user performs the operation to print scanned image data.
- **Storage / retrieval :**

  SFP for print data saved on an HDD or job data when the user saves the scanned image data to an HDD.

※Since this TOE does not incorporate the fax function, there is no operation and access control when "Fax send" or "Fax receive" is used. Also, since the print function from the network is not provided, there is no operation and access control in "Print".

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 or retrieval Job.*

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*]]

[assignment: *positive integer number*],

- 1

[assignment: *list of authentication events*]

- Refer to Table 6-4

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*]

- Refer to Table 6-4

[assignment: *list of actions*]

- Refer to Table 6-4

Table 6-4 Authentication failure handling

Authentication events	*Met, surpassed*	*List of actions]*
Administrator/User Authentication on the operation panel	Met	5-second suspension of certification
Administrator authentication in the Web Connection	Met	5-second suspension of certification

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*].

- Task attribute (User ID, Admin ID)
- Role (U.NORMAL, U.ADMIN)

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*]

- "-", "¥", "[", "]", ":", ";", ",", ". ", "/", """", """", "=", "~", "| ", "`", "{", "}", "+", "<", ">", "?" and "_" (administrator)
- "-", "¥", "[", "]", ":", ";", ",", ". ", "/", " ", """", "=", "~", "| ", "`", "{", "}", "+", "<", ">", "?" and "_" for general users

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***]

- Confirmation of TOE status and display settings
- Viewing the transmission history of scan data by scan operation, output history by copy operation, unoutput history that is the history of the job whose output was canceled, and output reservation for a job whose output was not completed

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*]

- Displaying the concealed character for each character of the entered character data

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* ***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***]

- Confirmation of TOE status and display settings
- Viewing the transmission history of scan data by scan operation, output history by copy operation, unoutput history that is the history of the job whose output was canceled, and output reservation for a job whose output was not completed

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*].

- Task attribute (User ID, Admin ID)
- Role (U.NORMAL, U.ADMIN)

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

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

- Associates with role U.ADMIN when authenticated with Admin ID (only one fixed)
- When authenticated by another ID, the role U.NORMAL is associated.

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

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

- None

6.1.5. Class FMT: Security management

FMT_MOF.1 **Management of security functions behaviour**

(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*]

- Refer to Table 6-5

[assignment: *list of functions*]

- Refer to Table 6-5

Table 6-5 Management of Security Functions behavior

Security Functions	Operations
Security enhancement setting function	Disable, enable
Service login permission setting function	Disable, enable
All data overwrite and delete function	Determine the behaviour of
Audit log destination setting function	Modify the behavior of
Trusted communications function	Modify the behavior of

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** 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]*]

- Refer to Table 6-6

[assignment: *list of security attributes*]

- Refer to Table 6-6

[assignment: *the authorized identified roles*]

- Refer to Table 6-6

Table 6-6 Management of Object Security Attribute

Security Attribute	Authorized Identified Roles	Operations
User ID	U.ADMIN	To register, modify, delete

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** 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 6-7, Table 6-8 and Table 6-9.**

Table 6-7 Operation of TSF Data (1)

TSF Data *owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL*

TSF Data	Operations	Authorized Roles
Login password for U.NORMAL	Modify	The owning U.NORMAL.
Login password for U.NORMAL	Registration and modification	U.ADMIN,

Table 6-8 Operation of TSF Data (2)

TSF Data *not owned by a U.NORMAL*

TSF Data	Operations	Authorized Roles
Date and time information	Modify	U.ADMIN
Encryption password	Modify	U.ADMIN

Password rule	Query, modify	U.ADMIN
U. ADMIN login password	Modify	U.ADMIN

Table 6-9 Operation of TSF Data (3)

TSF Data: *software, firmware, and related configuration data*

TSF Data	Operations	Authorized Roles
TOE firmware update data (firmware to be updated)	Modify	U.ADMIN

FMT_SMF.1 Specification of Management Functions

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

Hierarchical to : No other components

Dependencies : No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions provided by the TSF*].

~~Refinement~~

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

- refer to Table 6-10

Table 6-10 list of management functions

Management functions
Security enhancement setting function by U.ADMIN
Audit log destination setting function by U.ADMIN
User management function by U.ADMIN*.
Change own login password function by U.NORMAL
Change own login password function by U.ADMIN
Change date and time information function by U.ADMIN
Change password rules function by U.ADMIN
Registration and change of network settings function by U.ADMIN
Change encryption password function by U.ADMIN
Update firmware function by U.ADMIN
All data overwrite and delete function by U.ADMIN
Service login permission setting function by U.ADMIN

* User management functions include U.NORMAL login password management by U.ADMIN and subject security attribute management.

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 The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.

Refinement

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

6.1.6. Class FPT: Protection of the TSF

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 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_EXT.1 **Extended: Trusted Update**

(for O.UPDATE_VERIFICATION)

Hierarchical to : No other components

Dependencies : FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
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*]

- In the case of the operation panel,

  - ➢ For general users, the time determined by the auto-reset time after the last operation and the completion of processing by the last operation (1 minute when the auto-reset function is disabled).
  - ➢ For administrators, 30 minutes from the completion of processing by the last operation.
- For Web Connection, there is no interactive session

6.1.8. Class FTP: Trusted path/channels

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]

- File server (WebDAV, FTP, SMB)
- Audit log server (syslog)

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***]

- Electronic document transmission function
- Server sending function of the audit log

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**.

< Appendix B: 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_ENCRYPTION)

Hierarchical to : No other components.

Dependencies : [FCS_COP.1(e) Cryptographic operation (Key Wrapping),
FCS_SMC_EXT.1 Extended: Submask Combining,
FCS_COP.1(f) Cryptographic operation (Key Encryption),
FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or
FCS_COP.1(i) Cryptographic operation (Key Transport)]

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 encryption as specified in FCS_COP.1(f)

- 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_ENCRYPTION)

Hierarchical to : No other components

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

FDP_DSK_EXT.1.1 The TSF shall [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.

< Appendix D: Selection-based Requirements (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_ENCRYPTION)

Hierarchical to : No other components

Dependencies : [~~FDP_ITC.1 Import of user data without security attributes, or~~
~~FDP_ITC.2 Import of user data with security attributes, or~~
FCS_CKM.1(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*]

- CBC

[selection: *128 bits, 256 bits*]

- 256bits

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

- CBC as specified in ISO/IEC 10116

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

(selected from FCS_KYC_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_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(f) Refinement The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [[selection:** ***CBC, GCM*****] 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*****]**.

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

- CBC

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

- 256bits

[selection: ***CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772*****]**

- CBC as specified in ISO/IEC 10116

< Appendix D: Selection-based Requirements (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 : FIA_PSK_EXT.1 Extended:Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric Encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature Generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit

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* ~~(with mandatory support for NAT traversal as specified in section 2.23), 4307~~ *[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*]

- *RFC 4304 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 …

[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*

[assignment: *other DH groups that are implemented by the TOE*]

- none

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
- SHA-384
- SHA-512

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

- 160~512bits

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

- 160
- 256
- 384
- 512

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*]

- no other lengths

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
- SHA-512
- [assignment: method of conditioning text string]

[assignment: *method of conditioning text string*]

- SHA-384

[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 (Trusted Update) >

6.1.16. Class FCS: Cryptographic support

FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

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

Hierarchical to : No other components

Dependencies : No dependencies.

FCS_COP.1.1(c) 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***]

- SHA-1, SHA-256, SHA-384, SHA-512

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

6.1.17. Class FCS: Cryptographic support

FCS_PCC_EXT.1 Extended: Cryptographic Password Construct and Conditioning

(for O. STORAGE_ENCRYPTION)

Hierarchical to : No other components

Dependencies : FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)

FCS_PCC_EXT.1.1 A password used to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: *other supported special characters*]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [HMAC-[selection: *SHA-256, SHA384, SHA-512*]], with [assignment: *positive integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: *128, 256*] that meet the following: [**NIST SP 800-132**].

[assignment: *positive integer of 64 or more*]

- 64

[assignment: *other supported special characters*]

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

[selection: *SHA-256, SHA384, SHA-512*]

- SHA-256

[assignment: *positive integer of 1000 or more*]

- 1000

[selection: *128, 256*]

- 256

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
- a conditioned password submask

[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 800-132

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*]

- 512bit

FCS_SNI_EXT.1 Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

(selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)

Hierarchical to : No other components

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

FCS_SNI_EXT.1.1 The TSF shall only use salts that are generated by a RNG as specified in FCS_RBG_EXT.1.

FCS_SNI_EXT.1.2 The TSF shall only use unique nonces with a minimum size of [64] bits.

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner: [

- CBC: IVs shall be non-repeating,

- CCM: Nonce shall be non-repeating.

- XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer,

- GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.

].

6.2. Security assurance requirements

This section describes Security Assurance Requirements (SARs) for the TOE.

Table 6-11 TOE Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
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
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage

Tests	ATE_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

6.3. Security requirements rationale

6.3.1. The dependencies of security requirements

The dependencies between TOE security functional requirements are shown in the table below.

Table 6-12 The dependencies of security requirements

Functional requirements	Dependency relationship	ST-satisfied dependencies	Requirements that do not meet dependency
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A
FAU_GEN.2	FPT_STM.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	N/A
FAU_STG_EXT.1	FPT_STM.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1	N/A
FCS_CKM.1(a)	[FCS_COP.1(b), Or FCS_COP.1(i)] FCS_CKM_EXT.4	FCS_COP.1(b) FCS_CKM_EXT.4	N/A

FCS_CKM.1(b)	[FCS_COP.1(a),
	Or FCS_COP.1(d),
	Or FCS_COP.1(e),
	Or FCS_COP.1(f),
	Or FCS_COP.1(g),
	Or FCS_COP.1(h)]
	FCS_CKM_EXT.4
	FCS_RBG_EXT.1
		FCS_COP.1(a)
		FCS_COP.1(d)
		FCS_COP.1(e)
		FCS_COP.1(f)
		FCS_COP.1(g)
		FCS_COP.1(h)
		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)
		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)
		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.1(a) FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	For IPsec communication (FCS_IPSEC_EXT.1). In the case of the update function (FPT_TUD_EXT.1), FCS_CKM.1(a) and FCS_CKM_EXT.4 are not satisfied, but there is no problem because key generation is not performed.
FCS_RBG_EXT.1	No dependencies.	No dependencies.	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

Functional requirements	Dependency relationship	ST-satisfied dependencies	Requirements that do not meet dependency
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_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.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_EXT.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
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, And/or FCS_COP.1(i)]	FCS_COP.1(f)	N/A
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	N/A
FCS_COP.1(d)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A

Functional requirements	Dependency relationship	ST-satisfied dependencies	Requirements that do not meet dependency
FCS_COP.1(f)	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
	FCS_CKM.1(a)
	FCS_COP.1(a)
	FCS_COP.1(b)
	FCS_COP.1(c)
	FCS_COP.1(g)
	FCS_RBG_EXT.1
		FIA_PSK_EXT.1
		FCS_CKM.1(a)
		FCS_COP.1(a)
		FCS_COP.1(b)
		FCS_COP.1(c)
		FCS_COP.1(g)
		FCS_RBG_EXT.1
			N/A

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	-	Because bit-based pre-shared key generation using random bit generator is not selected.
FCS_COP.1(c)	No dependencies.	No dependencies.	N/A
FCS_PCC_EXT.1	FCS_COP.1(h)	FCS_COP.1(h)	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

FCS_SNI_EXT.1	FCS_RBG_EXT.1	FCS_RBG_EXT.1	N/A

7. TOE Summary specification

Table 7-1 shows a list of TOE's security functions derived from TOE's security function requirements. Details are described in the following sections.

Table 7-1 List of Security Functions

No.	Security function name
1	Identification and authentication function
2	Access control function
3	Storage encryption function
4	Trusted communications function
5	Security management function
6	Audit function
7	Software update verification function
8	Self-testing function

7.1. Identification and authentication function

FIA_UAU.1, FIA_UID.1

<Identification and Authentication of general users>

TOE acquires the user name and password from the user and performs identification and authentication by the main unit authentication method. Only those who are judged as authorized users as a result of verification are allowed to use TOE. The user enters the user name and password into TOE using the operation panel (when using Web Connection, this item does not apply because only the management function can be performed in Web Connection). TOE confirms that the registered username/password matches. Only the following operations can be performed before authentication is performed

- Checking the machine condition (the state of the reserved job, paper size in the paper tray, remaining quantity, etc.)
- Confirmation and modification of settings not related to the security function (settings related to printing, such as paper setting, image adjustment, and finisher position adjustment)
- Viewing the transmission history of scan data by scan operation, output history by copy operation, unoutput history that is the history of the job whose output was canceled, and output reservation for a job whose output was not completed

If the user performs the identification and authentication operation of the administrator while the user is permitted to use the TOE as a general user, the use of the TOE as a general user becomes impossible (logout) and the management function is permitted as another user. At the end of use of the management function, the TOE will not be available as the original general user.

<Identification and Authentication of Administrator>

Administrator identification and authentication mechanisms differ from those of general users.

In the operation panel or web browser (when using Web Connection), TOE asks the user to enter an administrator password when the user transitions to the screen where the management function can be used. The user who knows the administrator password is called the administrator. The user is not required to enter the user name here (the general user cannot combine the administrator positions) because the operation to be moved to the administrator setting screen is regarded as an identification. TOE acquires the administrator password from the user and performs identification and authentication by the main unit authentication method. Only those who are judged as the administrator as a result of the verification are allowed to use the TOE management function. The user enters the administrator password into TOE using the operation panel or the web browser (when using Web Connection). TOE confirms that the registered administrator password matches. No management function can be performed prior to the execution of identification and authentication.

In addition, when the user is allowed to use the management function, the identification and authentication operation cannot be performed as a general user (no means exists).

FIA_AFL.1

If authentication fails (once) for administrator and user authentication in the operation panel and administrator identification and authentication in the Web Connection, TOE will not perform the next authentication attempt on the user for five seconds.

FIA_PMG_EXT.1

TOE can set the following user password to combine uppercase and lowercase alphabetic characters, numbers, and the following special characters.

Table 7-2 Special Characters Available for Passwords

Special characters (32 characters) that can be used for an administrator password											
!	@	#	$	%	^	&	*	(	)	-	¥
[	]	:	;	,	.	/	"	'	=	~	|
`	{	}	+	<	>	?	_				

Special characters (32 characters) that can be used for general user passwords											
!	@	#	$	%	^	&	*	(	)	-	¥
[	]	:	;	,	.	/	Space	'	=	~	|
`	{	}	+	<	>	?	_				

When a user sets or changes the user password listed below, TOE checks whether the number of characters of the new password is equal to or greater than the minimum number of characters for password (the minimum number of characters for password is set by the administrator to a range of 8 to 64 characters). If the condition is not met, the setting is not reflected and a message requesting reset is displayed.

- Administrator password
- User password

FIA_USB.1

The TOE is associated with the user identifier (User ID) and role U.NORMAL with the task to be executed on behalf of the user after user identification and authentication. After the administrator's identity is authenticated, the Admin ID and the role U.ADMIN are associated with the task to be performed on behalf of the user. Since tasks on behalf of users are associated with each interface, identification and authentication of general users and administrators can be performed from the operation panel during administrator identification and authentication in the Web Connection (only the firmware version can be confirmed in the Web Connection).

FIA_UAU.7

When a user enters a password for authentication from the operation panel or web browser, TOE displays dummy characters (*) corresponding to the number of input characters instead of the entered characters.

FTA_SSL.3

The TOE terminates the session when a user who has been identified and authenticated in the operation panel or Web Connection meets the following conditions.

- In the case of the operation panel, general users will be logged out one minute after the completion of processing by the last operation is completed (when the auto-reset function is disabled) or after the set auto-reset time (can be set between 1 and 9 minutes). The administrator will also be logged out 30 minutes after the completion of processing by the last operation is completed, and will be required to re-authenticate.
- For Web Connection, identification and authentication is successful and logs out immediately after the browser displays the firmware version.

7.2. Access control function

FDP_ACC.1, FDP_ACF.1

Based on the user data access control described in Table 6-2 and Table 6-3, TOE restricts users from using user document data and user job data. Access to each data can only be performed using the operation panel.

(1) Restricting operations on user document data and user job data when using the operation panel

- When switching to the screen where the scan, copy, storage and retrieval functions are performed on the operation panel, identification and authentication to TOE is requested, and each function cannot be used without authentication. At this time, the administrator password cannot be logged in (functions cannot be used).
- User ID is recorded as owner information in the creation of user job data and user document data.
- After authentication, the administrator can display the list of HDD storage jobs (thumbnail image, file name, last update date, etc. on the first page of the job) and delete each job by the general user on the administrator setting screen. In addition, by setting the storage job automatic deletion period, it is possible to delete the saved job after a certain period. Modify cannot be executed for user document data and user job data stored on an HDD because I/F does not exist.
- Job owner can be a Read, Modify, Delete for user document data and user job data stored on the HDD. In the HDD Save Job List screen, the function to save/fetch a job and the output reservation of a job whose output has not been completed can be displayed. Only jobs that can be operated by the login user are displayed in this screen and other user-owned jobs are not displayed. That is, since I/F does not exist, the function to save/retrieve other user-owned jobs cannot be executed. Output reservation for jobs that have not completed output cannot be executed because there is no I/F for Read, Modify, or Delete.
- Job owner can delete user document data and user job data created by copy operation by clicking the Stop button. However, even in Job owner, Read and Modify of user document data created by copy operation and Modify of user job data cannot be executed because I/F is not present.
- Even with Job owner, Read, Modify, Delete of user document data created by scanning operation, Modify, and Delete of user job data cannot be executed because I/F is not present.
- Transmission history of scan data by scan operation, output history by copy operation, non-output history of the job whose output was canceled, and output reservation of the job whose output was not completed can be viewed by anyone, including unauthenticated users.

FIA_ATD.1

The TOE defines the task attributes (User ID, Admin ID) and roles (U.NORMAL, U.ADMIN) of the tasks on behalf of the user as attributes.Task attribute and role allocation timing are as follows.

- General User: When an administrator registers a user from the operation panel, U.NORMAL is assigned a unique User ID as a user attribute and a fixed role
- Administrator: Administrator has only one Admin ID and cannot be added or deleted. U.ADMIN is assigned as a fixed role

7.3. Storage encryption function

The storage device encryption function is enabled by the encryption library embedded in the main unit control firmware after TOE startup, and the encrypted area of each device cannot be accessed when it is disabled. Data is encrypted before writing to the device, and data is decrypted after reading from the device. This process is performed on all encrypted target data to be written to/read from each device. The material protection function of the encryption key used for encryption is described in detail below.

FCS_COP.1(d), FCS_KYC_EXT.1, FCS_COP.1(f), FCS_CKM.1(b), FPT_SKP_EXT.1, FCS_PCC_EXT.1, FCS_KDF_EXT.1, FCS_COP.1(h), FPT_KYP_EXT.1,FCS_SNI_EXT.1,FCS_COP.1(c)

TOE implements cryptographic algorithms in accordance with the following standards. When executing the random bit generation process using CTR_DRBG, a bit string of 1024 bits is generated from the software entropy source, and the random number is generated by inputting the bit string into the random bit generation function of the library software (GUARD FIPS Security Toolkit) in the firmware.

Table 7-3 Cryptographic algorithm

Algorithm	Standard	SFR Reference
CTR_DRBG	NIST SP 800-90A	FCS_RBG_EXT.1
PBKDF2	NIST SP 800-132	FCS_KDF_EXT.1 FCS_PCC_EXT.1
HMAC-SHA-256	ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2" ISO/IEC 10118	FCS_COP.1(h)

AES-CBC 256bits	ISO/IEC 10116	FCS_COP.1(d)
		FCS_COP.1(f)

TOE generates the encryption keys described in Table 7-4 to achieve storage encryption.

Table 7-4 Encryption Key for Storage Encryption

Key type	Overview
DEK(256bit)	Used for data encryption on storage devices. Generated by executing random bit generation in accordance with CTR_DRBG (AES-256) in the TOE manufacturing process.
KEK(256bit)	Used for encryption when storing DEK.

When using TOE, administrators are guided to register and generate KEK by executing "Encryption password Setting Function". This function can also be used to regenerate KEK. In this function, the following processing is performed by the administrator by resetting the encryption password.

(1) A key derivation function is used to generate a KEK from the key material stored in QSPI Flash.
(2) Read encrypted DEK from QSPI Flash, decrypt it with the above key, and expand it to RAM.
(3) Based on the password set by the user, a new 256-bit KEK is generated by the password-based key derivation function (PBKDF2) of the encryption library incorporated into this control firmware. The parameters at the time of derivation are as follows.

- Using SHA-256 (in accordance with ISO/IEC 10118-3:2004) according to PRF:HMAC-SHA-256 *FCS_COP.1(c)
- Password: encryption password (64 characters) set by the user from the operation panel
  ※ It can be set to a combination of uppercase and lowercase alphabets, numbers, and special characters (see Table 7-5).The maximum length is 64 characters.If there are less than 64 characters, they will be left-justified as null padding.
- Salt: 384-bit random number generated by the random number generator described in TSS of FCS_RBG_EXT.1
  ※ The value obtained from the software entropy source (1024 bits) is used as the Entropy Input (1024 bits) and the obtained random number is used.
- IterationCount: 1000 times
- IV: There is no corresponding parameter in PBKDF2..

(4) Encrypt DEK with newly generated KEK.
(5) Store the key material (password/Salt) and encrypted DEK at KEK derivation in QSPI Flash.

Table 7-5 Special characters (32 characters) that can be used for the password

Special characters (32 characters) that can be used for encryption passwords											
!	@	#	$	%	^	&	*	(	)	-	¥
[	]	:	;	,	.	/	"	'	=	~	|
`	{	}	+	<	>	?	_				

The encryption key generated by the above-mentioned means is used in the initialization process at TOE startup as follows.

(1) When the TOE's sub power supply is turned on, the bootloader starts and reads and executes each firmware from the SSD's firmware storage area.
(2) The TOE firmware reads the key material (password and Salt) from the QSPI Flash and derives the key using the password-based key derivation function (PBKDF2).
(3) Read the encrypted DEK from the QSPI Flash, decrypt it with the re-derived KEK, and expand it to RAM.
(4) The TOE firmware decrypts the setup information stored in SSD and NVRAM using the decrypted DEK, initializes all functions including the TOE security functions, and displays the basic screen on the operation panel after completion to make the TOE functions available to users.

As shown above

- KEK keys are not stored on media corresponding to NVRAM, QSPI Flash, or portable storage media, but are stored only in RAM. The key material is stored on a QSPI Flash on the substrate, but not on a medium that corresponds to a portable storage medium.
- The DEK key is stored in the encrypted state in the QSPI Flash on the TOE board, but is not stored in the medium corresponding to the portable storage medium. There is no key material.
- The decrypted DEK key is stored in RAM only. It is not stored on media that corresponds to portable storage media.
- There is no external interface to access both the key and the key material of KEK/DEK.

Thus, the encryption key is considered to be protected.

FDP_DSK_EXT.1

TOE encrypts data using the encryption key described in Table 7-4.

In TOE, the device capable of holding encrypted user document data and confidential TSF data is an SSD/HDD that is a portable storage medium and an NVRAM/QSPI Flash that is not a portable storage medium (TSF data on RAM is erased with sub power off). Only the devices listed here are not subject to encryption because they do not handle TSF information or do not have the ability to hold TSF data when the sub power is OFF. Table 7-6 and Table 7-7 show the data to be encrypted for each device.

Table 7-6 Data to be encrypted for each device (portable storage medium)

Storage	Contents and areas	Encryption support method	Encryption key	Algorithm	Encryption conditions
SSD	SSD system area (partition table, etc.)	No encryption target	-	-	-
	Storage of firmware	No encryption target	-	-	-
	TOE Setting Information Storage Area (Set value saved by administrator)	Encrypted file system	DEK	AES(CBC)	Every minute
	SWAP area (disabled)	Not used	-	-	-
	Controller area (TOE network setting, destination server address, password)	Encrypted file system	DEK	AES(CBC)	Every minute
	Control area (authentication data)	Encrypted file system	DEK	AES(CBC)	Every minute
	Audit log information	Encrypted file system	DEK	AES(CBC)	Every minute
HDD (RAID 0)	Job storage area (job management data/job blog)	Proprietary implementation	DEK	AES(CBC)	Every minute
	Job storage area (image data, thumbnails)	Proprietary implementation	DEK	AES(CBC)	Every minute

Table 7-7 Data to be encrypted for each device (other than portable storage media)

Device	Contents and areas	Encryption support method	Encryption key	Algorithm	Encryption conditions
NVRAM	TOE setting information storage area (password information excluding user authentication, scan function destination/audit log destination setting)	Encrypt and save password information (Plaintext if the area does not fall under the above)	DEK	AES(CBC)	Every minute
QSPI Flash	DEK	Encrypted and saved	KEK	AES(CBC)	Every minute
	KEK key material	As plaintext	-	-	-

The items described in Table 7-6 and Table 7-7 are described.

- The encrypted file system is a file system software that manages the read/write of all files of the partition (area) described as "encrypted file system" in the encryption support method column and performs encryption and decryption processing without fail. There is no interface that can avoid encryption and decryption processing. Encryption by the encrypted file system is enabled in the TOE manufacturing process at Konica Minolta's plant (DEK keys are generated and used in the encrypted file system). Therefore, the administrator does not need to activate the encryption function (there is no way to disable it).

- The "job storage area (job management data/job blog)" of the HDD is encrypted and decrypted using the interface responsible for job management data input/output. Since the job management data performs all the read/write operations using the above interface, and the encryption and decryption processes are performed without fail, there is no interface that can avoid encryption and decryption processes. Encryption processing by the job management data I/O interface is enabled in the TOE manufacturing process at Konica Minolta's factories (DEK keys are generated and used in the job management data I/O interface). Therefore, the administrator does not need to activate the encryption function (there is no way to disable it).
- The "job storage area (image data/thumbnail)" of the HDD is encrypted and decrypted using the interface responsible for image data input/output. Since the image data is read/Write by the above-mentioned interface and encryption/decryption processing is always performed, there is no interface that can avoid encryption/decryption processing. Encryption processing using the image data I/O interface is enabled in the TOE manufacturing process at Konica Minolta's plant (DEK keys are generated and used in the job management data I/O interface). Therefore, the administrator does not need to activate the encryption function (there is no way to disable it).
- The "storage area of the firmware" of the SSD is the area where encryption is not performed. The corresponding area is read/Write by the OS standard file system, but the interface for direct file access to the user is not provided.

FCS_RBG_EXT.1

TOE implements a CTR DRBG (AES-256) conforming to NIST SP 800-90A and an RBG consisting of a single software noise source. The above CTR DRBG uses the Derivation Function and Reseed,, but the Prediction Resistance function does not work. The software noise source implements a condition branch code or the like that affects the internal state of the CPU and a clock counter value acquisition process in the loop process. The variation of the loop processing execution time is acquired through the clock counter to obtain the raw data. Conditioning is performed to agitate and compress the entropy included in the raw data into the entire bit using shift operations and XOR, and after increasing the entropy rate of the entire bit, it is output as an entropy value.

TOE uses this RBG to generate a random number and uses it to generate the key material of the encryption key KEK and the key key DEK (key length: 256 bits). When the TOE generates a random number, if the CTR DRBG requires a seed material (Entropy Input and Nonce), start the software to be used as the noise source and obtain and use the required size entropy value. This entropy value satisfies the minimum amount of entropy required for Instantiate and Reseed (in the case of TOE, 256 bits equal to the security strength) shown in 10.2.1 of NIST SP800-90A and contains sufficient entropy.

FCS_CKM.4, FCS_CKM_EXT.4

In TOE, the key material of the cryptographic key KEK used for the storage encryption function is stored in the QSPI Flash, which cannot be exchanged locally, and used to protect each data including setting information related to the basic control of TOE regardless of the security enhancement settings. Table 7-8 shows KEK and DEK key storage locations and the timing of their destruction.

The administrator is advised to perform the all data overwrite and delete function when the TOE is discarded with guidance.

Table 7-8 Storage and destruction of keys

Key		Storage location	Timing of destruction	Method of destruction
KEK	Key material	QSPI Flash	Time of TOE destruction	Deleted by 0x00 once.
	Key generated from the key material by the key derivation function	RAM	When the key is not required (when the TOE sub power is turned off)	Deleted from RAM due to TOE sub power off
DEK	Key (encrypted state)	QSPI Flash	Time of TOE destruction	Deleted by 0x00 once.
	Key (plaintext)	RAM	When the key is not required (when the TOE sub power is turned off)	Deleted from RAM due to TOE sub power off

7.4. Trusted communications function

FPT_SKP_EXT.1

All pre-shared keys, symmetric keys, and private keys used in the TOE's trusted communications function are stored in the controller area of the RAM and SSD. The SSD controller area is protected by an encrypted file system (see TSS for storage encryption function for details). In addition, there is no interface for accessing cryptographic keys stored in RAM and SSD.

Thus, the encryption key is considered to be protected.

FCS_CKM.1(a)

TOE generates an RSA asymmetric key with a key length of 2048 bits in the method described in the rsakpg1-crt method described in Section 6.3.1.3 of NIST SP800-56B, Revision 2 in the generation of IPsec certificates used for key establishment of IPsec communication by PKI setting of Web Connection. Also, in the key establishment for IPsec communication (see FTP_ITC.1), an asymmetric key is generated by Diffie-Hellman Group 14 as described in the Using the Approved Safe-Prime Groups described in Section 5.6.1.1.1 of NIST SP800-56A, Revision 3.

FCS_CKM.1(b)

The TOE generates a random number using the RBG described in FCS_RBG_EXT.1 and generates a 128-bit or 256-bit symmetric encryption key at the start of IPsec communication (see FTP_ITC.1) or at the key establishment after the SA lifetime. TOE invokes the above RBG by calling the DRBG function (CTR DRBG (AES-256)) and generates a random number.

FCS_RBG_EXT.1

TOE implements a CTR DRBG (AES-256) conforming to NIST SP 800-90A and an RBG consisting of a single software noise source. The above CTR DRBG uses the Derivation Function and Reseed,, but the Prediction Resistance function does not work. The software noise source implements a condition branch code or the like that affects the internal state of the CPU and a clock counter value acquisition process in the loop process. The variation of the loop processing execution time is acquired through the clock counter to obtain the raw data. Conditioning is performed to agitate and compress the entropy included in the raw data into the entire bit using shift operations and XOR, and after increasing the entropy rate of the entire bit, it is output as an entropy value.

If the CTR DRBG requires a seed material (Entropy Input and Nonce) when the TOE generates a random number, start the software to be used as the noise source and obtain and use the required size entropy value. This entropy value satisfies the minimum amount of entropy required for Instantiate and Reseed (in the case of TOE, 256 bits equal to the security strength) shown in 10.2.1 of NIST SP800-90A and contains sufficient entropy.

FCS_COP.1(a)

TOE uses an AES-CBC with a key length of 128 bits and 256 bits conforming to FIPS PUB 197 and NIST SP 800-38A as an ESP cryptographic algorithm for IPsec communication. The IKEv1 cryptographic algorithm uses an AES-CBC with a key length of 128 bits and 256 bits that conform to FIPS PUB 197 and NIST SP 800-38A.

FTP_TRP.1(a)

TOE performs encrypted communication in communication with other reliable IT devices. The following functions are subject to encryption communication.

Table 7-9 Reliable path (FTP_TRP.1(a)) available to the administrator

Recipient of communication	Contents and functions of the communication to be encrypted	Protocol
Client PC	Use of Web Connection by browser	IPsec

FTP_ITC.1

TOE performs encrypted communication with IT devices. The encrypted communication provided by TOE is as follows. (When security enhancement setting is enabled)

Table 7-10 Encrypted communication provided by TOE

Recipient of communication	Protocol	Cryptographic algorithms	Associated interface
File server (FTP)	IPsec	AES(128bits、256bits)	Execute scan function from the operation panel
File server (WebDAV)	IPsec	AES(128bits、256bits)	Execute scan function from the operation panel
File server (SMB)	IPsec	AES(128bits、256bits)	Execute scan function from the operation panel
Audit log server (syslog)	IPsec	AES(128bits、256bits)	See Table 7-14

FCS_IPSEC_EXT.1, FCS_COP.1(g), FCS_COP.1(b), FCS_COP.1(c)

In the IPsec protocol used by TOE, the following settings are available and no other settings are available. Multiple items are items that can be selected by the administrator. Only the administrator can set or change this item.

- IPsec Encapsulation Settings: Transport Mode
- Security Protocol: ESP
  - ESP cryptographic algorithm: AES_CBC-128, AES_CBC-256
  - ESP authentication algorithm: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512

    ※By the above selection, message digest length is 160 bits and 160 bits HMAC-SHA-1, message digest length is 256 bits and 256 bits HMAC-SHA-256, message digest length is 384 bits and 384 bits HMAC-SHA-384, and message digest length is 512 bits and 512 bits of HMAC-SHA-512, and message authentication code (HMAC) is used to communicate using keyed hashing.

    ※The hash algorithm uses SHA-1, SHA-256, SHA-384, and SHA-512 (conforming to ISO/IEC 10118-3:2004) according to FCS_COP.1(c).

    ※ESP supports extended sequence number (ESN).
- Key Exchange Method: IKEv1

<Setting with IKEv1>

  - IKEv1 cryptographic algorithm: AES_CBC-128, AES_CBC-256
  - IKEv1 authentication algorithm: SHA-1, SHA-256, SHA-348, SHA-512 compliant with ISO/IEC 10118-3:2004
  - Negotiation mode: Main Mode

  - Phase 1 (main mode) key valid time: 600 to 86,400 seconds
  - Phase 2 (Quick mode) Key validity time: 600 to 28,800 seconds
  - Diffie-Hellman Group: Group 14
- Peer authentication method: digital signature (according to RSA digital signature algorithm (rDSA) 2048 bits, FIPS PUB 186-4, "Digital Signature Standard"), hash algorithm: SHA-256 (according to ISO/IEC 10118-3:2004), pre-shared key

The TOE implements the IPsec Security Policy Database (SPD) and the following settings can be made by the administrator.

- IPsec Policy: Allows administrator to specify the conditions of IP packets and select the action to be taken (protect, pass, or discard) for IP packets that meet each condition. IPsec policy can be set up to 10 groups (IP policy group 1-10), and is applied to both sending and receiving packets. When multiple IPsec policies are set for one communication partner, regardless of the registration order of IPsec policy groups 1-10, the operation is applied in the following priority order.

  Priority: High protection > Discard > Passage priority: Low
- Default Action: Select from the following options what to do if there are no settings that match IPsec policy. (Guidance is given to the administrator to choose to destroy this setting.)
  - Discard: Discard IP packets that do not match the IPsec policy setting
  - Passing: Passing IP packets that do not match the IPsec policy setting

FIA_PSK_EXT.1

The TOE uses the following text-based pre-shared key as the pre-shared key for IPsec. The text-based prior shared key is converted into a bit string using the hash algorithm described below.

- Text-based pre-shared key
  - Length: 22 characters
  - Available Characters: strings of ASCII characters (combining uppercase and lowercase alphabetic characters, numeric characters, and special characters ("!", "@", "#", "$", "%"%", "&", "*", "(", ")")")), or HEX Values
  - Conditioning Methods: SHA-1, SHA-256, SHA-384, and SHA-512

FCS_CKM.4, FCS_CKM_EXT.4

In TOE, the encryption keys used for the trusted communications function and their key materials are stored in the controller area of the SSD or in the RAM, and are used for key exchange, authentication, or encryption of communications at the time of establishing the secure communication. Table 7-11 shows the storage destination of keys and keys used for IPsec communication and the method of destruction. The pre-shared key set by the administrator and the private key of the IPsec certificate are stored on the SSD, and the timing when it becomes unnecessary is limited to when the TOE is discarded. Guidance indicates that all data overwrite and delete function should be performed by the administrator when the TOE is discarded. In the all data overwrite and delete function, the encryption key and the key material storage area are overwritten once with a fixed value (0). Session keys (temporary encryption keys) used in IPSec etc. are stored in RAM. These items are deleted because they are no longer needed when the TOE sub power is turned off.

Table 7-11 Destination and Destination of Key

Key	Storage destination	Timing of destruction	Method of destruction
IPsec certificate key pair	SSD	When the TOE is destroyed.	Deleted by 0x00
IPsec pre-shared key	SSD	When the TOE is destroyed.	Deleted by 0x00
IPsec cookie/nonce	RAM	When a key is not required (when the TOE sub-power supply is turned off)	Deleted from RAM due to TOE sub-power shutdown
Shared secret key for IKE (generated in IKEv1 Phase 1)	RAM	When a key is not required (when the TOE sub-power supply is turned off)	Deleted from RAM due to TOE sub-power shutdown
Shared secret key for IPsec (Generated in IKEv1 Phase 2)	RAM	When a key is not required (when the TOE sub-power supply is turned off)	Deleted from RAM due to TOE sub-power shutdown
IPsec Diffie-Hellman common key	RAM	When a key is not required (when the TOE sub-power supply is turned off)	Deleted from RAM due to TOE sub-power shutdown

7.5. Security management function

FMT_MOF.1, FMT_SMF.1, FIA_UID.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1

TOE provides users with the following management functions. Each management function is operable only from the interface described. When switching to the screen where the following management functions are executed on the operation panel, identification and authentication to TOE is requested, and the management function cannot be used without authentication. Upon successful identification and authentication, the user is associated with a role (U.ADMIN, U.NORMAL) and allowed to use the functions provided for each role. In addition, the associated role is retained until logout. TOE assigns the User ID of the user who created the user document data and user job data as the Job owner in the access control of Table 6-2 and Table 6-3. TOE does not have the function to overwrite the assigned User ID.

Table 7-12 Administrative functions provided to U.ADMIN

Management function	Description	Permitted operations	Operable interface
Security enhancement setting function	Enable/disable security enhancement settings.	Change	Operation panel
Audit log destination setting function	Set audit log transmission (network setting such as IP address of destination server).	Change	Operation panel
User management	U.ADMIN can register, modify, or delete users with a User ID (including the function to set the login password for U.NORMAL by U.ADMIN). The user data access control described in Table 6-2 and Table 6-3 is used for user registration to set the appropriate initial value for the attribute.	To modify, delete, and create	Operation panel
U.ADMIN login password change function	U.ADMIN changes the password of U.ADMIN.	Change	Operation panel

Management function	Description	Permitted operations	Operable interface
Function to change the date and time information	Set the date and time information.	Change	Operation panel
Password rule modification function	Set and change the Password rule (the minimum number of characters for password setting).	Change	Operation panel
Registering and modifying network settings	Set and change network settings (e.g., IP address of TOE, IP address of DNS server, port number, NetBIOS name, IPsec setting, etc.).	Change	Operation panel
Function to set and change the encryption password	Set and change the encryption password that is the data underlying the encryption key (KEK) used in the storage encryption function.	Change	Operation panel
Firmware update function	Execute firmware update of TOE.	Execution	Operation panel
All data overwrite and delete function	Overwrite the encryption key and key material storage area once with a fixed value (0).	Execution	Operation panel
Service login permission setting function	Allow/disable service mode	Change	Operation panel

Table 7-13 Administrative functions provided to U.NORMAL

Management function	Description	Permitted operations	Operable interface
Function to set the login password of U.NORMAL	U.NORMAL sets its own login password.	Change	Operation panel

7.6. Audit function

TOE generates and records an audit log for the event being audited and sends it to the log server.

FAU_GEN.1, FAU_GEN.2

The TOE defines the following events as the event to be audited and records the event occurrence time (month, day, hour, second), event type, subject identification information, and event results.

Table 7-14 List of Audited Events

Event to be audited	ID (Subject Identification Information *1)	Results	Associated interface
Executing administrator authentication	Admin ID	OK/NG	FIA_UAU.1, See FIA_UID.1
Changing/registering administrator password	Admin ID	OK	See Table 7-12
Executing user authentication	User ID/unregistered ID	OK/NG	FIA_UAU.1, See FIA_UID.1
Creation of users by administrators	Admin ID	OK	See Table 7-12
Changing/registering user passwords by administrator	Admin ID	OK	See Table 7-12
Deleting a user by administrator	Admin ID	OK	See Table 7-12
Changing user attributes by administrator	Admin ID	OK	See Table 7-12

Event to be audited	ID (Subject Identification Information *1)	Results	Associated interface
Changing user attributes by user (e.g. changing user password)	User ID	OK	See Table 7-13
Changing security enhancement settings	Admin ID	OK/NG	See Table 7-12
Changing Password rule settings	Admin ID	OK	See Table 7-12
Changing network settings	Admin ID	OK	See Table 7-12
Changing service login permission settings.	Admin ID	OK	See Table 7-12
Changing the destination settings for the audit log	Admin ID	OK	See Table 7-12
Changing the HDD encryption password	Admin ID	OK	See Table 7-12
Executing the firmware update function (ISW)	Admin ID	OK/NG	See Table 7-12
Executing firmware diagnosis	Admin ID/unregistered ID	OK/NG	See FPT_TST_EXT.1
Setting Date and Time	Admin ID	OK	See Table 7-12
Starting the Audit Function	Unregistered ID	OK	Secondary power supply
Termination of the audit function	Unregistered ID	OK	Secondary power supply
Deleting stored jobs	User ID / Admin ID	OK	See FDP_ACC.1 and FDP_ACF.1
Printing a copy job	User ID	OK/NG	See FDP_ACC.1 and FDP_ACF.1
Saving a copy job	User ID	OK/NG	See FDP_ACC.1 and FDP_ACF.1
Executing a Scan Job	User ID	OK/NG	See FDP_ACC.1 and FDP_ACF.1
Printing stored jobs	User ID	OK/NG	See FDP_ACC.1 and FDP_ACF.1
Modify/Restore (Move/Replicate) Save Job	User ID	OK/NG	See FDP_ACC.1 and FDP_ACF.1
Reading a Save Job	User ID	OK/NG	See FDP_ACC.1 and FDP_ACF.1
Failure to establish an IPsec session	Unregistered ID	ErrNo(*2)	See FTP_ITC.1

(*1) The fixed value of unregistered ID as subject identification information is recorded for the subject event that occurred before identification and authentication.

(*2) Records error information indicating the cause of the IPsec session failure

FAU_STG_EXT.1

Recorded audit log information is retained in the TOE and then log files are transmitted according to the external audit server (syslog) set by the administrator. See Table 7-15 for the log transmission timing.

Table 7-15 Audit Log Information Specifications

Handling of audit log information	Overview
Storage area of log information	SSD area encrypted with storage encryption function
Log information transmission timing	When the event to be audited occurs (immediately)
Log information to be sent	Log information about the event that occurred

Processing in case of transmission failure	When log information cannot be sent to the log server due to network failure, etc., it is temporarily saved in SSD (*1). Up to 10,000 cases. The subsequent information is discarded when the log information reaches 10,000. The temporarily saved information is transmitted when communicating with the server, and the information on the SSD is deleted.

It is temporarily stored in the log storage area on the SSD shown in (*1) Table 7-6. The stored information is protected from unauthorized access by encrypting it in the file system. For details, refer to TSS of FDP_DSK_EXT.1. In addition, the TOE does not provide a user interface for accessing the storage area of log information, so there is no means for reading out log information.

FPT_STM.1

TOE has a clock function and provides only the administrator with the function to change the time of TOE. Time information to be recorded in the audit log is provided by the clock function.

7.7. Software update verification function

FPT_TUD_EXT.1

TOE only grants administrators the following functions.

- Firmware version check function
- Firmware update function

The administrator can verify the firmware version in the Configure After Identification screen or in the web browser after authentication from the Web Connection.

The administrator can execute the firmware update function on the administrator setting screen after authentication. When executing firmware update, TOE verifies firmware files using the digital signature of Konica Minolta included in the firmware file as a program check after data transfer. The FW is rewritten only when it is determined that there is no problem as a result of the verification. If the digital signature verification fails (at this time, the hash value of the firmware is calculated and the hash value is stored in the encrypted file system of the SSD. This hash value data is used for the self-testing function described below), the TOE displays a warning on the operation panel and stops the update process.

FCS_COP.1(b), FCS_COP.1(c)

TOE verifies firmware files using digital signature verification as follows.

1. Firmware files include digital signature data and firmware data. Digital signature data conform to RSA digital signature algorithm (rDSA) 2048 bit, FIPS PUB 186-4, "Digital Signature Standard".
2. Decrypts the digital signature data with the public key of TOE.
3. The data decrypted above is compared with the firmware data calculated by SHA-256 in accordance with ISO/IEC 10118-3:2004. The firmware data is judged to be normal if it matches.

7.8. Self-testing function

FPT_TST_EXT.1

When TOE is sub powered on, firstly, firmware self-test is performed in the order of main control firmware and network control firmware, and then FW is read. The hash value of the main control firmware and the network control firmware, which control security functions, is calculated, and the existence of falsification is detected by checking the match with the hash value data recorded on the SSD during the firmware verification, and the integrity of the TSF execution code is verified. Since the encryption library used in TOE at this time is also subject to hash value verification, integrity is also verified. If the verification fails, the TOE displays a warning (SC code) on the operation panel and stops the operation and moves to the state where the operation is not accepted. Firmware other than the above is excluded from the firmware verification function because they do not have access to TSF data and security function execution capability and do not have access to TSF data.

If the verification fails, the TOE displays a warning (SC code) on the operation panel and stops the operation and moves to the state where the operation is not accepted.

This is sufficient to demonstrate that the TSF is operating correctly because the above process can confirm the integrity of the firmware that determines the behavior of the TSF.