

TOSHIBA

e-STUDIO330AC/400AC

Models with FAX unit and FIPS Hard Disk

Security Target

Version 1.04

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

TABLE OF CONTENTS

1. ST INTRODUCTION	1
1.1. ST Reference.....	1
1.2. TOE Reference.....	1
1.3. TOE Overview	1
1.4. TOE Description	4
1.4.1. Physical Boundary	4
1.4.2. Guidance	6
1.4.3. Logical Boundary	7
1.4.3.1. General Functions	7
1.4.3.2. Security Function.....	8
1.4.3.3. Terminology	9
2. CONFORMANCE CLAIM	10
2.1. CC Conformance Claim	10
2.2. PP Conformance Claim	10
2.3. Package Conformance Claim.....	10
2.4. Conformance Rationale	10
3. SECURITY PROBLEM DEFINITIONS	11
3.1. Users	11
3.2. Assets	11
3.2.1. User Data.....	11
3.2.2. TSF Data	12
3.3. Threats	12
3.4. Organization Security Policies	13
3.4.1. Organizational Security Policy Definitions.....	13
3.5. Assumption Definitions	13
4. SECURITY OBJECTIVES	14
4.1. Security Objectives for Operational Environment	14
5. EXTENDED COMPONENT DEFINITIONS	15
5.1. FAU_STG_EXT Extended: External Audit Trail Storage.....	15
5.2. FCS_CKM_EXT Extended: Cryptographic Key Management	15
5.3. FCS_HTTPS_EXT Extended: HTTPS selected.....	16
5.4. FCS_KDF_EXT Extended: Cryptographic Key Derivation	17

5.5.	FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)	18
5.6.	FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)	19
5.7.	FCS_SMC_EXT Extended: Submask Combining	20
5.8.	FCS_TLS_EXT Extended: TLS selected	20
5.9.	FDP_DSK_EXT Extended: Protection of Data on Disk	22
5.10.	FDP_FXS_EXT Extended: Fax Separation	23
5.11.	FIA_PMG_EXT Extended: Password Management	23
5.12.	FPT_KYP_EXT Extended: Protection of Key and Key Material	24
5.13.	FPT_SKP_EXT Extended: Protection of TSF Data	25
5.14.	FPT_TST_EXT Extended: TSF testing	26
5.15.	FPT_TUD_EXT Extended: Trusted Update	26
6.	SECURITY REQUIREMENTS	28
6.1.	Notation	28
6.2.	Class FAU: Security Audit	28
6.2.1.	FAU_GEN.1 Audit data generation	28
6.2.2.	FAU_GEN.2 User identity association	28
6.2.3.	FAU_STG_EXT.1 Extended: External Audit Trail Storage	29
6.3.	Class FCS: Cryptographic Support	29
6.3.1.	FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)	29
6.3.2.	FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)	29
6.3.3.	FCS_CKM.4(a) Cryptographic key destruction	30
6.3.4.	FCS_CKM.4(b) Cryptographic key destruction	30
6.3.5.	FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction	30
6.3.6.	FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)	30
6.3.7.	FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)	31
6.3.8.	FCS_RBG_EXT.1(a) Extended: Cryptographic Operation (Random Bit Generation)	31
6.3.9.	FCS_RBG_EXT.1(b) Extended: Cryptographic Operation (Random Bit Generation)	31
6.3.10.	FCS_COP.1(c) Cryptographic operation (Hash Algorithm)	31
6.3.11.	FCS_COP.1(f) Cryptographic operation (Key Encryption)	32
6.3.12.	FCS_SMC_EXT.1 Extended: Submask Combining	32
6.3.13.	FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)	32
6.3.14.	FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)	32
6.3.15.	FCS_TLS_EXT.1 Extended: TLS selected	32
6.3.16.	FCS_HTTPS_EXT.1 Extended: HTTPS selected	33
6.3.17.	FCS_KDF_EXT Extended: Cryptographic Key Derivation	33
6.3.18.	FCS_KYC_EXT.1 Extended: Key Chaining	33
6.4.	Class FDP: User Data Protection	34
6.4.1.	FDP_ACC.1 Subset access control	34

6.4.2. FDP_ACF.1 Security attribute based access control	37
6.4.3. FDP_FXS_EXT.1 Extended: Fax separation	37
6.4.4. FDP_DSK_EXT.1 Extended: Protection of Data on Disk	38
6.5. Class FIA: Identification and Authentication.....	38
6.5.1. FIA_AFL.1 Authentication failure handling	38
6.5.2. FIA_ATD.1 User attribute definition	38
6.5.3. FIA_PMG_EXT Extended: Password Management	38
6.5.4. FIA_UAU.1 Timing of authentication	39
6.5.5. FIA_UAU.7 Protected authentication feedback.....	39
6.5.6. FIA_UID.1 Timing of identification.....	39
6.5.7. FIA_USB.1 User-subject binding.....	39
6.6. Class FMT: Security Management	40
6.6.1. FMT_MOF.1 Management of security functions behavior.....	40
6.6.2. FMT_MSA.1 Management of security attributes	40
6.6.3. FMT_MSA.3 Static attribute initialization.....	41
6.6.4. FMT_MTD.1 Management of TSF data.....	41
6.6.5. FMT_SMF.1 Specification of Management Functions	42
6.6.6. FMT_SMR.1 Security roles	46
6.7. Class FPT: Protection of the TSF	46
6.7.1. FPT_SKP_EXT.1 Extended: Protection of TSF Data	46
6.7.2. FPT_STM.1 Reliable time stamps	46
6.7.3. FPT_TST_EXT.1 Extended: TSF testing	46
6.7.4. FPT_TUD_EXT.1 Extended: Trusted Update	46
6.7.5. FPT_KYP_EXT.1 Extended: Protection of Key and Key Material	47
6.8. Class FTA: TOE Access.....	47
6.8.1. FTA_SSL.3 TSF-initiated termination.....	47
6.9. Class FTP: Trusted Paths/Channels	47
6.9.1. FTP_ITC.1 Inter-TSF trusted channel	47
6.9.2. FTP_TRP.1(a) Trusted path (for Administrators).....	47
6.9.3. FTP_TRP.1(b) Trusted path (for Non-administrators)	48
6.10. Security Assurance Requirements	48
6.11. Security Functional Requirements Rationale.....	49
6.11.1. Dependencies of Security Functional Requirements Documents	49
6.11.2. Security Assurance Requirements Rationale	51
7. TOE SUMMARY SPECIFICATION.....	52
7.1. Audit.....	52
7.2. Cryptographic Support.....	54
7.3. Storage Encryption (Conditionally mandatory).....	57

- 7.4. Storage Encryption (Selective requirements).....59
- 7.5. Communication Protection (Selective requirements)60
- 7.6. Trusted Update (Selective requirements)62
- 7.7. User Data Protection62
- 7.8. PSTN Fax-Network Separation.....68
- 7.9. Identification and Authentication.....69
- 7.10. Security Management.....70
- 7.11. Protection of the TSF.....73
- 7.12. TOE Access75
- 7.13. Trusted Path/Channel.....75

- APENDIX..... 78

List of Tables

Table 1	TOE Configuration Item	1
Table 2	Guidance	6
Table 3	Terminology	9
Table 4	User Categories.....	11
Table 5	User Data types.....	11
Table 6	TSF Data types	12
Table 7	Threats	12
Table 8	Organization Security Policies.....	13
Table 9	Assumptions.....	13
Table 10	Security Objectives for the Operational Environment.....	14
Table 11	Auditable Events.....	28
Table 12	D.USER.DOC Access Control SFP	34
Table 13	D.USER.JOB Access Control SFP	36
Table 14	Other Available Characters.....	39
Table 15	Security Attributes List.....	40
Table 16	Management of TSF Data.....	41
Table 17	Management Functions	42
Table 18	Time Interval of User Inactivity.....	47
Table 19	TOE Security Assurance Requirements.....	48
Table 20	Analysis Results of Dependencies for Security Functional Requirements.....	49
Table 21	Recorded Events and Audit Logs.....	52
Table 22	Print Access Control for D.USER.DOC	62
Table 23	Scan Access Control for D.USER.DOC	63
Table 24	Copy Access Control for D.USER.DOC	64
Table 25	Fax Transmission Access Control for D.USER.DOC	64
Table 26	Fax Reception Access Control for D.USER.DOC.....	65
Table 27	Print Access Control for D.USER.JOB	66
Table 28	Scan Access Control for D.USER.JOB.....	66
Table 29	Copy Access Control for D.USER.JOB	67
Table 30	Fax Transmission Access Control for D.USER.JOB.....	67
Table 31	Fax Reception Access Control for D.USER.JOB	68
Table 32	Definition of TSFI	76
Table 33	Definition of Acronyms	78

List of Tables

Figure 1	Environment for the usage of the MFP	2
Figure 2	Physical Boundary.....	4
Figure 3	Logical Boundary.....	7

1. ST Introduction

ST Reference, TOE Reference, TOE Overview, and TOE Description are described in this Chapter.

1.1. ST Reference

The identity of the ST is described below.

Title: TOSHIBA e-STUDIO330AC/400AC Models with FAX unit and FIPS Hard Disk Security Target
Version: 1.04
Date Created: August 25, 2020
Author: TOSHIBA TEC CORPORATION

1.2. TOE Reference

The identity of the TOE is described below.

TOE Name: TOSHIBA e-STUDIO330AC/400AC Models with FAX unit and FIPS Hard Disk
Version: SYS V1.0
TOE Type: Digital Multi-functional Peripherals
Developer Name: TOSHIBA TEC CORPORATION

The TOE shown above is consists of the MFP and required option as shown in **Table 1**.

Table 1 TOE Configuration Item

Required components	Identification information of TOE	Sales Area
MFP	• Model Number e-STUDIO330AC or e-STUDIO400AC • Version SYS V1.0	North America
FAX unit	GD-1370NA-N	
FIPS Hard Disk kit GE-1230	MQ01ABU032BW	
MFP	• Model Number e-STUDIO330AC or e-STUDIO400AC • Version SYS V1.0	Europe
FAX unit	GD-1370EU	
FIPS Hard Disk kit GE-1230	MQ01ABU032BW	

1.3. TOE Overview

1.3.1. TOE Type

The TOE is the Multi-functional Peripherals that work in a network environment and provide capabilities of print, copy, scan, and fax.

1.3.2. Usage and Major Security Features of the TOE

The TOE defined in the ST is the Digital Multi-functional Peripherals with the following basic functions.

- Copy function
- Printer function

- Scan function
- Fax function

The Fax function will be available by installing the option GD-1370NA-N, or GD-1370EU. The TOE provides the following security features.

- Authorization for using the identification, authentication, and HCD functions
- Audit
- Access control
- Encryption
- Reliable communication
- Administrator's role
- Reliable operation
- Separation of PSTN fax and network

1.3.3. Required Non-TOE Hardware and Software

The TOE is assumed to be installed in a general office and used in a network environment. Also, it is assumed to be used by being connected with the client PC and the server within the network (LAN) that is protected from unauthorized access from the external network by a firewall. Figure 1 shows the hardware other than the TOE and the operational environment.

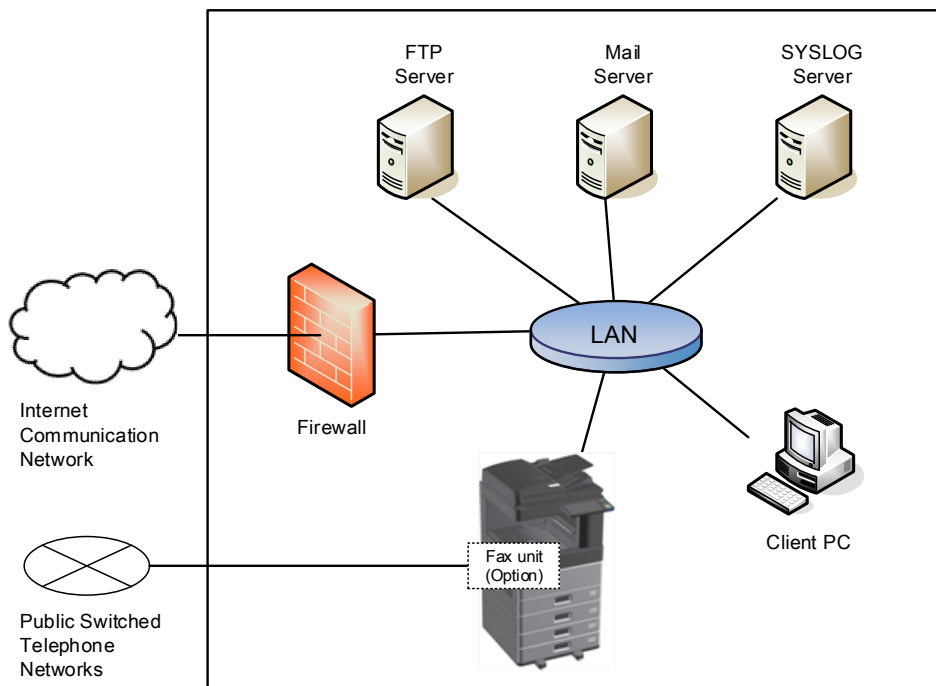


Figure 1 Environment for the usage of the MFP

- Client PC

U.NORMAL(a) can request printing of the document data through the LAN to the TOE. The U.ADMIN(a) can refer to or change the setting data in the MFP using the Web browser. The configuration of browser and Client Utility Software is as follows:

- Web browser: Internet Explorer 11
- Printer Driver: TOSHIBA Universal Printer Driver2 (Version: 7.212.4835.14)

- Mail Server

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

- Fire Wall

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

- FTP Server

The FTP Server is a server which activates the File Transfer Protocol Server Software. The TOE and the FTP Server is connected with TLS communication.

- SYSLOG Server

The SYSLOG Server is a server which transmits/receives TOE log data which is transferred using the Syslog protocol. The TOE and the SYSLOG Server is connected with TLS communication.

- Printer Driver

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

1.4. TOE Description

1.4.1. Physical Boundary

The TOE is the Digital Multi-functional Peripherals (e-STUDIO330AC, e-STUDIO400AC) consists of hardware and software. The physical boundary is as shown below. The MFP is delivered to users by a transport service provider with being packed in a cardboard box

Hardware Construction

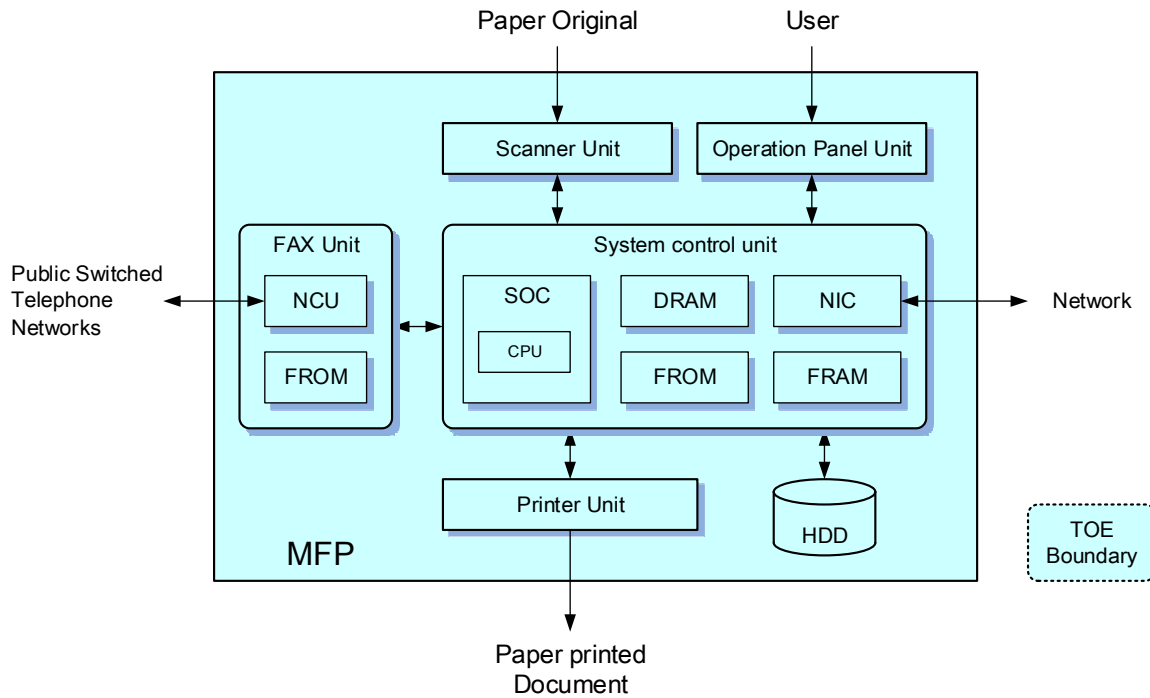


Figure 2 Physical Boundary

Software Construction

- SYSTEM FIRMWARE: Ver. TP01SF0W1504
- SYSTEM SOFTWARE: Ver. TP01HD0W1504
- ENGINE FIRMWARE: Ver. TH440MWW07
- SCANNER FIRMWARE: Ver. TH440SLGWW05
- FAX1 FIRMWARE: Ver. FAXH625TA12

• Control Panel Unit

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

• Scanner Unit

The Scanner Unit is an input device which scans paper original and transmits the image data to the System Control Unit. Firmware (SCANNER FIRMWARE) which controls communication between the Scanner Unit and the System Control Unit is stored in the HDD.

• Control Panel Unit

The Control Panel Unit is a user interface by which a U.USER operates the MFP. Hardware

construction is operation buttons, LEDs, and LCD with a touch panel. Information from the MFP is displayed on the LCD and each operation such as copy start is executed by communicating with the System Control Unit.

- Printer Unit

The Printer Unit is a unit which receives a print request from the System Control Unit and prints the print data on the paper. Firmware (ENGINE FIRMWARE) which controls communication between the Printer Unit and the System Control Unit is stored in the FROM in the Printer Unit.

- HDD (FIPS Hard Disk Kit: GE-1230)

The HDD is a Hard Disk Drive with the self-encryption function complies with the Federal Information Processing Standard (FIPS140-2) in the US and a required Option Unit with JCMVP authentication (JCMVP authentication No.: F0022). Not only a part of software (SYSTEM SOFTWARE) that controls the MFP, but also image data and document data is stored. The protection assets data is saved to an encrypted partition. The FIPS Hard Disk Kit is delivered to a user by a transport service provider with being packed in a cardboard box.

- FROM (Flash Memory)

The FROM is a nonvolatile storage memory. A part of software (SYSTEM FIRMWARE) that controls the MFP is stored.

- FRAM

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

- SoC

SoC is a LSI in which a device controller circuit is integrated with a microprocessor at the core, and is a semiconductor chip which performs basic control of the MFP behavior.

- DRAM

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

- NIC (Network Interface Card)

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

- Fax Unit (GD-1370NA-N/GD-1370EU)

The Fax Unit is a required option unit which connects to the PSTN and transmits/receives fax documents between the Fax devices which comply with G3. The PSTN circuit standard differs depending on the sales countries and areas. So, an appropriate fax option is selected for each area. The identifier is distinguished by the trailing alphabet (NA-N, EU) of the model number as shown in Table 1. The same firmware (FAX FIRMWARE) regardless of the sales countries and areas which controls Fax communication and communication between the System Control Units is stored in the FROM in the Fax Unit for each destination, and all users can use the same fax functions. The fax option is delivered to the users by a transport service provider with being packed in a cardboard box.

1.4.2. Guidance

There are two types of the TOE Guidance written in English and Japanese as shown in **Table 2** and **Table 3**; One is stored in the DVD-ROM in the PDF format and the other is supplied as a printed document. The Japanese version and English version are delivered to Japan and the other countries respectively together with the MFP. For the Fax Option Guidance, the Japanese version and the English version are packed as a printed document in GD-1370NA-N and GD-1370EU respectively.

Table 2 Guidance

Title	Identifier	PDF Format	Print
Quick Start Guide	OME19001200	✓	✓
Safety Information	OME170056C0	✓	✓
Copying Guide	OME170060B0	✓	
Scanning Guide	OME170066C0	✓	
MFP Management Guide	OME170074D0	✓	
Software Installation Guide	OME170072C0	✓	
Printing Guide	OME170070C0	✓	
TopAccess Guide	OME170076D0	✓	
Software Troubleshooting Guide	OME170062B0	✓	
Hardware Troubleshooting Guide	OME170048B0	✓	
High Security Mode Management Guide	OME170078C0	✓	
Paper Preparation Guide	OME170046B0	✓	
Specifications Guide	OME170058C0	✓	
Fax Guide GD-1370	OME170080D0	✓	

1.4.3. Logical Boundary

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

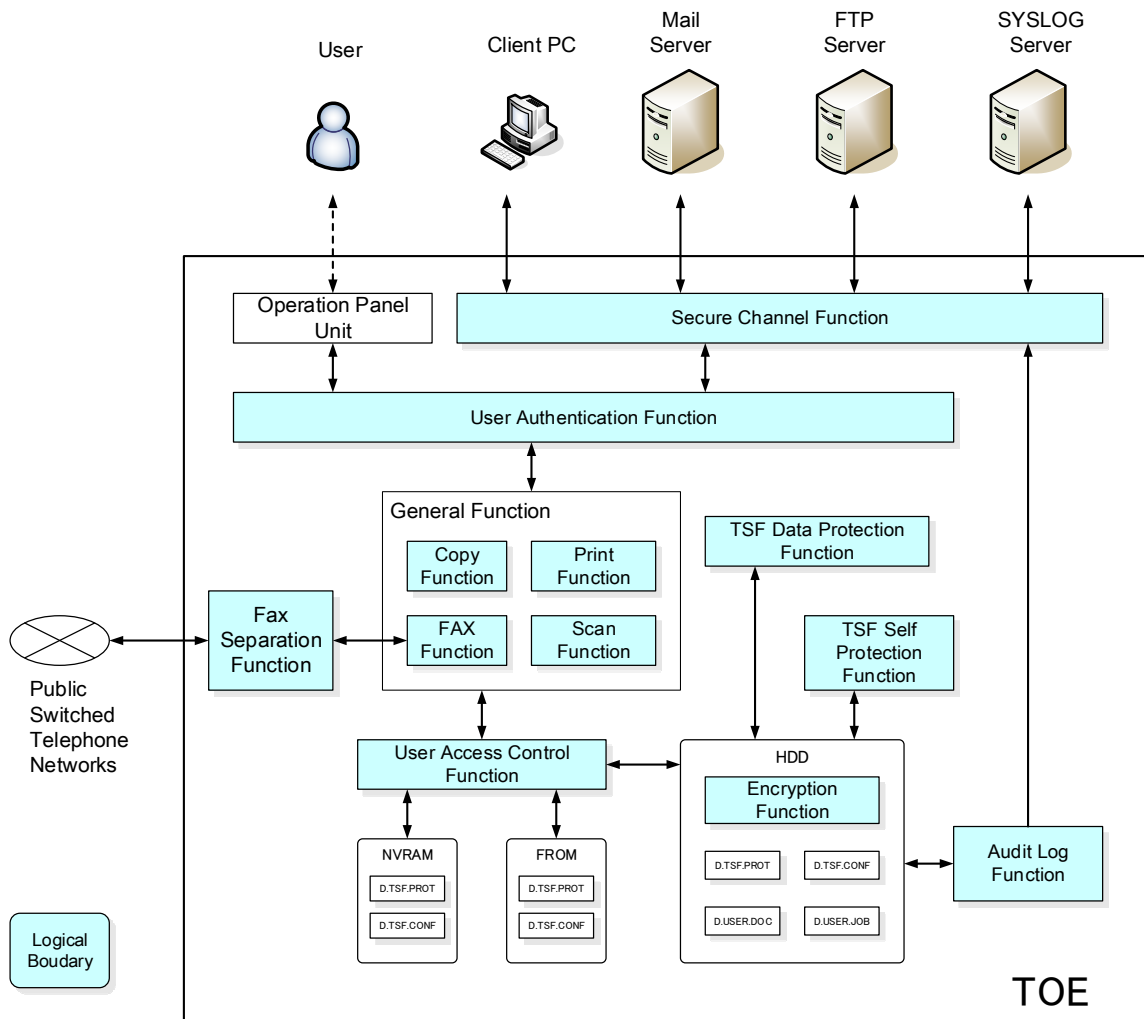


Figure 3 Logical Boundary

1.4.3.1. General Functions

The TOE is provided with a series of functions associated with images, such as Copy, Print, and Scan, as the General Functions, and controls these functions integrally.

- Copy function

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

- Print function

A Print function is a function which transmits the print data from the client PC to the TOE through the LAN and prints the data on a paper.

- Scan function

The Scan function can attach and send a paper document by user operation on the control panel and reading the paper document with the Scanner to an email and the FTP server.

- Fax function

The Fax function consists of the Fax transmission function and the Fax reception function. The Fax transmission function is a function which transmits the paper document data read with the Scanner Unit to the external Fax machine through the PSTN. The Fax reception function is a function which receives the document data transmitted from the external Fax machine through the PSTN. In order to achieve the above functions, the Fax option (GD-1370NA-N, or GD-1370EU) is required.

1.4.3.2. Security Function

The security functions provided by the TOE are as follows:

- Function which gives permission to use the identity, authentication, and HCD functions

It is a function which verifies whether a user who wants to use the TOE is an authorized user, and gives the user a permission to use the TOE only when the user is identified. The TOE prompts a user to enter the user ID and user password from the control panel or the client PC for user authentication, and has the feedback protection function which displays dummy characters during user password entry and the lockout function which locks a user who failed in authentication out.

- Access Control Function

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

- Audit Function

The TOE generates audit logs for tracking the state of the TOE. All logs recorded per event are transferred to the audit server and viewable from the audit server.

- Trusted Communication Function

The TOE supports the cryptographic communication protocol in order to prevent communication data from being leaked or tampered on the network during connection and communication with the LAN. The TOE communicates with the client PC, mail server, SYSLOG server, and FTP server in the operational environment using TLS for data encryption. The TOE protects the print data by using TLS and print protocol IPPS during communication with the client PC when IPP print is performed by the client PC using the printer driver.

- TSF Self Protection

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

- TSF Data Protection

The function that only the administrator authenticated by the identification and authentication function can perform operations related to TSF data from the operation panel or TopAccess. For example, you can change the date and time, register/delete users, enable or disable available services and protocols.

- Data Encryption

The Data Encryption is a function to encrypt user data saved in the HDD to protect them from

being leaked.

- Function which separate PSTN Fax and Network

This function prevents access from the phone line to the LAN by restricting entry from PSTN to Fax reception.

- Software Update Verification

This function is a function which verifies whether software to be updated is authorized when software of the TOE is updated.

1.4.3.3. Terminology

The terms which are defined by CC and PP in Chapter 2 out of the specific terms associated with the ST should follow the definition thereof. The other terms are defined as shown in **Table 3**.

Table 3 Terminology

Terminology	Definition
User ID	An identifier given to a general user and MFP administrator. The TOE specifies the user by the identifier.
User Password	A password which is used to log into the TOE by a user.
Job Log	The job information such as Print Job, Transmission Journals, Reception Journals and Scan Job.
Message Log	Logs regarding MFP's device information or operations executed by users.
TopAccess	A web-based job and device control tool. The MFP information can be retrieved by using this tool through network.
Auto Logout Time	Time to log out when a logged in user does not operate the MFP for a certain period of time.
Lockout Time	Time until the locked out account is released.
Date and Time	Time information for log management. Year/moth/day/hour/min/sec
Role	U.NORMAL, U.ADMIN U.NORMAL is detailed in U.NORMAL(a) and U.FAXOPERATOR. U.ADMIN is detailed in U.ADMIN(a), U.ACCOUNTMANAGER, U.ADDRESSBOOKOPERATOR.
Firmware	Software which is embedded into the device to control hardware.
Cipher Suite	Combination of the cryptographic algorithms used for TLS communication, which consists of the combination of "Key replacement_Signature_Encryption_Hash function".
Address Book	Fax numbers and email addresses can be registered and displayed in the destination list. It enables simple specification of the fax transmission destinations and scan email transmission destinations.
User Authentication Failure Handling	An administrator can change the number of retries for entering the login password and lockout time and clear the locked out account status.
Secure Channel	A communication channel in which data is encrypted to prevent wiretapping by the third party.
European Special Characters	Words with the German umlauts and French cedilla.

2. Conformance Claim

2.1. CC Conformance Claim

The following shows the CC Conformance Claim of the ST and TOE.

Common Criteria version: Version 3.1 Release 5

- Part1: Introduction and general model April 2017 Version 3.1 Revision 5
- Part2: Security functional components April 2017 Version 3.1 Revision 5
- Part3: Security assurance components April 2017 Version 3.1 Revision 5
- Conformance of ST to CC part2: CC part 2 Extended
- Conformance of ST to CC part3: CC part 3 Conformant

2.2. PP Conformance Claim

The ST and TOE conform to the following PP.

PP Name: Protection Profile for Hardcopy Devices
PP Version: 1.0 dated September 10, 2015
Recognition Identification: JISEC-C0553
Errata: Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

2.3. Package Conformance Claim

The ST does not conform to the packages

2.4. Conformance Rationale

The following conditions requested by PP have been satisfied and must be “Exact Conformance” as requested by PP. Therefore, the TOE type is consistent with PP.

- Required Uses
Printing, Scanning, Copying, Networking communications, Administration
- Conditionally Mandatory Uses
PSTN faxing, Fileld-Replaceable Nonvolatile Storage
- Optional Uses
None

3. Security Problem Definitions

3.1. Users

The User and role of the TOE are defined as shown below in the ST.

Table 4 User Categories

Designation		Category name	Definition
U.NORMAL A User who has been identified and authenticated and does not have an administrative role	U.NORMAL(a)	Normal User	A User who is authorized to execute Copy, Print, Scan, and Fax functions which are the basic functions of the TOE. A general user is authorized to operate each function and can execute only the authorized function
	U.FAXOPERATOR	Normal User	A user who can execute the Fax transmission/reception functions
U.ADMIN A User who has been identified and authenticated and has an administrative role	U.ADMIN(a)	Administrator	An administrator who is authorized to manage the entire TOE, such as setting of the TOE security functions, change of the user account information, and browse of the audit log
	U.ACCOUNTMANAGER	Administrator	An administrator who can perform the settings for the user account management (setting of the user ID and role of the user and operation authority of the basic functions)
	U.ADDRESSBOOKOPERATOR	Administrator	A user who can edit the address book

3.2. Assets

3.2.1. User Data

The two User Data is defined in the ST.

Table 5 User Data types

Designation	User Data type	Definition	Details
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form	Copy Document Data
			Print Document Data
			Scan Document Data
			Fax Transmission Document Data
			Fax Reception Document Data
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job	Print Job
			Scan Job
			Copy Job
			Fax Transmission Job
			Fax Reception Job

3.2.2. TSF Data

The TSF Data consist of the following 2 types.

Table 6 TSF Data types

Designation	User Data type	Definition	Details
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	Enable/Disable of the Secure Channel
			User ID
			Role
			Allowable Number of entry for Login Password
			Lockout Time
			Locked Account Status
			Auto Logout Time
			Date and Time Information
			Minimum Password Length
			Address Book
			SYSLOG Server Settings
			FTP Server Settings
			Software update
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	User Password
			Encryption Key

3.3. Threats

The Threats to the TOE which are countered by the conforming products are as shown below.

Threats are defined by a threat agent that performs an action resulting in an outcome that has the potential to violate TOE security policies.

Table 7 Threats

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

3.4. Organization Security Policies

The following are Organizational Security Policies³ (OSPs) that are upheld by conforming products.

3.4.1. Organizational Security Policy Definitions

Organizational Security Policies are used to provide a basis for Security Objectives that are not practical to define on the basis of Threats to Assets or that originate primarily from customer expectations.

Table 8 Organization Security Policies

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

3.5. Assumption Definitions

Assumptions are conditions that must be satisfied in order for the Security Objectives and functional requirements to be effective.

Table 9 Assumptions

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 Operational Environment

The details of the Security Objectives for the Operational Environment are as described in **Table 10**.

Table 10 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 Component Definitions

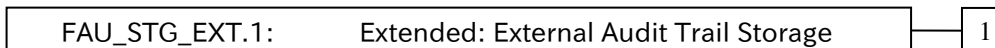
Extended component definitions are listed below.

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 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 audits 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.

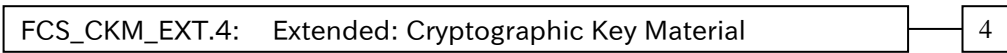
This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

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 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

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.

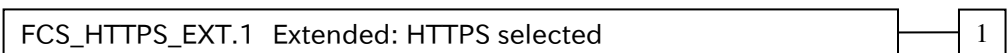
This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.3. FCS_HTTPS_EXT Extended: HTTPS selected

Family Behavior:

Components in this family define requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

Component leveling:



FCS_HTTPS_EXT.1 HTTPS selected, requires that HTTPS be implemented according to RFC 2818 and supports TLS.

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 of HTTPS session establishment

FCS_HTTPS_EXT.1 Extended: HTTPS selected

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Rationale:

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

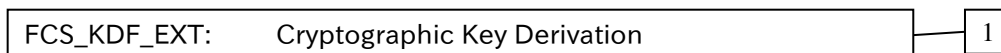
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.4. FCS_KDF_EXT Extended: Cryptographic Key Derivation

Family 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.1 Extended: Cryptographic Key Derivation

Hierarchical to: No other components.

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

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

Rationale:

The TSF is required to specify the means by which an intermediate key is derived from a specified set of submasks using the specified hash functions.

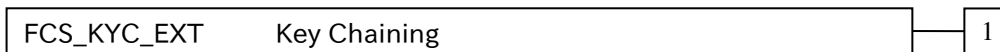
This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key chains, and it is therefore placed in the FCS class with a single component.

5.5. FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family 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(i) Cryptographic operation (Key Transport),
 FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation),
 and/or
 FCS_COP.1(f) Cryptographic operation (Key Encryption)].

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: *one, using a submask as the 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.

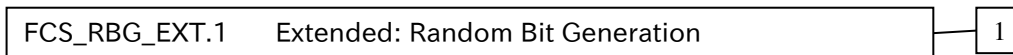
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] *software-based noise source(s)*, [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: 128 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security strength table for hash functions”, of the keys and hashes that it will generate.

Rationale:

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

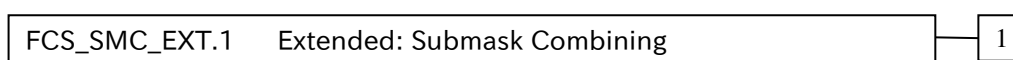
This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.7. FCS_SMC_EXT Extended: Submask Combining

Family Behavior:

This family defines the means by which submasks are combined, if the TOE supports more than one submask being used to derive or protect the BEV.

Component leveling:



FCS_SMC_EXT.1 Submask combining requires the TSF to combine the submasks in a predictable fashion.

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_SMC_EXT.1 Extended: Submask Combining

Hierarchical to: No other components.

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

FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [selection: exclusive OR (XOR), SHA-256, SHA-512] to generate an intermediary key or BEV.

Rationale:

Submask Combining is to ensure the TSF combine the submasks in order to derive or protect the BEV.

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

5.8. FCS_TLS_EXT Extended: TLS selected

Family Behavior:

This family addresses the ability for a server and/or a client to use TLS to protect data between a client and the server using the TLS protocol.

Component leveling:

FCS_TLS_EXT.1	Extended: TLS selected	1
---------------	------------------------	---

FCS_TLS_EXT.1 TLS selected, requires the TLS protocol 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 of TLS session establishment

FCS_TLS_EXT.1 Extended: TLS selected

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: *TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[selection:

- None
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384]

Rationale:

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

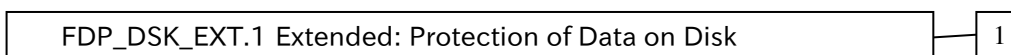
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.9. 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.

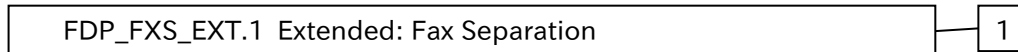
This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

5.10. FDP_FXS_EXT Extended: Fax Separation

Family Behavior:

This family addresses the requirements for separation between Fax PSTN line and the LAN to which TOE is connected.

Component leveling:



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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FDP_FXS_EXT.1 Extended: Fax separation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

Fax Separation is to protect a LAN against attack from PSTN line, and the Common Criteria does not provide a suitable SFR for the Protection of TSF or User Data.

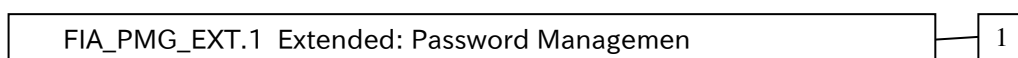
This extended component protects the TSF Data or User Data, and it is therefore placed in the FDP class with a single component.

5.11. 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 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.

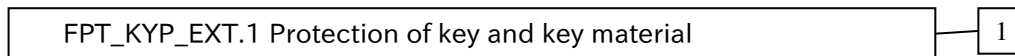
This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KYP_EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device, and not store any such plaintext key on a device that uses the key for its encryption.

Rationale:

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

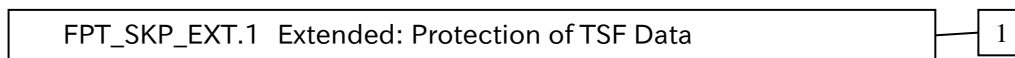
This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

5.13. 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.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

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

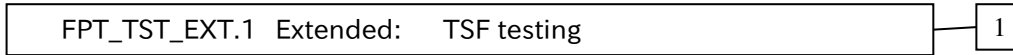
This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.14. 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.

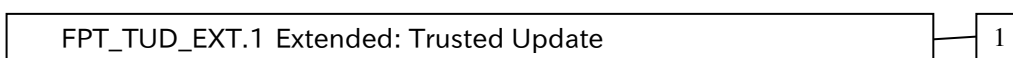
This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

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 Trusted Update

Hierarchical to: No other components.

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

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

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

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: 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

6.1. Notation

- **Bold** typeface indicates the portion that has been “completed” or “refined” in this PP.
- ***Bold italic*** typeface indicates the portion that has been “assigned”, “selected” or “refined” in this ST.
- Letters in brackets indicate the “assigned” or “selected” results.
- SFR components that are followed by a letter in parentheses, e.g., (a), (b)⋯ represent required iterations.

6.2. Class FAU: Security Audit

6.2.1. FAU_GEN.1 Audit data generation

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

- Start-up and shutdown of the audit functions;
- All auditable events for the **not specified** level of audit; and
- All auditable events specified in Table 11, [none].**

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 11, [none].**

Table 11 Auditable Events

Auditable events	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure

6.2.2. FAU_GEN.2 User identity association

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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

6.2.3. 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.

6.3. Class FCS: Cryptographic Support

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

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/ verification)
FCS_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 [

- *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.

6.3.2. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(a) Cryptographic Operation (Symmetric 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 [128 bit, 256 bit]** that meet the following: **No Standard.**

6.3.3. FCS_CKM.4(a) 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(a) Refinement: The TSF shall **destroy** cryptographic keys in accordance with a specified cryptographic key **destruction** method [

For volatile memory, the destruction shall be executed by *[powering off a device]*.

For nonvolatile storage, the destruction shall be executed by a *[single]* overwrite of key data storage location consisting of *[a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1)]*, followed by a *[none]*. If read-verification of the overwritten data fails, the process shall be repeated again;
] that meets the following: *[no standard]*.

6.3.4. FCS_CKM.4(b) 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(b) Refinement: The TSF shall **destroy** cryptographic keys in accordance with a specified cryptographic key **destruction** method [

For volatile memory, the destruction shall be executed by *[powering off a device]*.

For nonvolatile storage, the destruction shall be executed by a *[three]* overwrite of key data storage location consisting of *[a static pattern]*, followed by a *[none]*. If read-verification of the overwritten data fails, the process shall be repeated again;
] that meets the following: *[no standard]*.

6.3.5. 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.

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

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

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

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

- FIPS PUB 197, “Advanced Encryption Standard (AES)”
- [NIST SP 800-38A, NIST SP 800-38D]

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

(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic key generation]

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

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

(for O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1(b) The TSF shall perform all deterministic random bit generation services in accordance with [NIST SP 800-90A] using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2(b) The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [single] hardware-based noise source(s) with a minimum of [128bits] 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.

6.3.10. 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 [SHA-1, SHA-256, SHA-384, SHA-512] that meet the following: [ISO/IEC 10118-3:2004].

6.3.11. 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 *[[CBC] mode]*** and cryptographic key sizes [**256 bits**] that meet the following: [**AES as specified in ISO /IEC 18033-3, *[CBC as specified in ISO/IEC 10116]***].

6.3.12. FCS_SMC_EXT.1 Extended: Submask Combining

(selected in FCS_KYC_EXT.1.1)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(c) Cryptographic operation (Hash Algorithm)
FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [**exclusive OR (XOR)**] to generate an intermediary key or BEV.

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

(selected with FCS_IPSEC_EXT.1.4)

Hierarchical to: No other components.

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

FCS_COP.1.1(g) Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-**[SHA-1, SHA-256]**, key size [**160, 256**]bits, and message digest sizes [**160, 256**] bits that meet the following: FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."

6.3.14. 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: 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 [**HMAC-SHA-512**] and cryptographic key sizes [256] that meet the following: [**ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"**; ISO/IEC 10118].

6.3.15. FCS_TLS_EXT.1 Extended: TLS selected

(selected in FDP_ITC.1.1, FDP_TRP.1.1)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric Keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[

- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_SHA256*

].

6.3.16.FCS_HTTPS_EXT.1 Extended: HTTPS selected

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6.3.17.FCS_KDF_EXT 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 [*a RNG generated submask as specified in FCS_RBG_EXT.1*] to derive an intermediate key, as defined in [*NIST SP 800-108 [KDF in Counter Mode]*], 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.

6.3.18.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(i) Cryptographic operation (Key Transport),
FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation),
and/or FCS_COP.1(f) Cryptographic operation (Key Encryption)].

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

6.4. Class FDP: User Data Protection

6.4.1. FDP_ACC.1 Subset access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **Table 12** and **Table 13**.

Table 12 D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	<i>Operation:</i>	<i>Submit a document to be printed</i>	<i>View image or Release printed output</i>	<i>Modify stored document</i>	<i>Delete stored document</i>
	Job owner	(note 1)		denied	
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied
Scan	<i>Operation:</i>	<i>Submit a document for scanning</i>	<i>View scanned image</i>	<i>Modify stored image</i>	<i>Delete stored image</i>
	Job owner	(note 2)			
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied

Copy		"Create"	"Read"	"Modify"	"Delete"
		<i>Operation:</i>	<i>Submit a document for copying</i>	<i>View scanned image or Release printed copy output</i>	<i>Modify stored image</i>
	Job owner	(note 2)		denied	
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send		<i>Submit a document to send as a fax</i>	<i>View scanned image</i>	<i>Modify stored image</i>	<i>Delete stored image</i>
	Job owner	(note 2)			
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR		denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive		<i>Receive a fax and store it</i>	<i>View fax image or Release printed fax output</i>	<i>Modify image of received fax</i>	<i>Delete image of received fax</i>
	Job owner	(note 3)		denied	
	U.ADMIN(a)	(note 4)		denied	
	U.NORMAL(a)	(note 4)	denied	denied	denied
	U.ACCOUNTMANAGER	(note 4)	denied	denied	denied
	U.FAXOPERATOR	(note 4)		denied	
	U.ADDRESSBOOKOPERATOR	(note 4)	denied	denied	denied
	Unauthenticated	(note 4)	denied	denied	denied

Table 13 D.USERJOB Access Control SFP

Print		"Create" *	"Read"	"Modify"	"Delete"
	<i>Operation:</i>	<i>Create print job</i>	<i>View print queue / log</i>	<i>Modify print job</i>	<i>Cancel print job</i>
Print	Job owner	(note 1)		denied	
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated		denied	denied	denied
Scan		"Create" *	"Read"	"Modify"	"Delete"
	<i>Operation:</i>	<i>Create scan job</i>	<i>View scan status / log</i>	<i>Modify scan job</i>	<i>Cancel scan job</i>
Scan	Job owner	(note 2)		denied	
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy		"Create" *	"Read"	"Modify"	"Delete"
	<i>Operation:</i>	<i>Create copy job</i>	<i>View copy status / log</i>	<i>Modify copy job</i>	<i>Cancel copy job</i>
Copy	Job owner	(note 2)			
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send		"Create" *	"Read"	"Modify"	"Delete"
	<i>Operation:</i>	<i>Create fax send job</i>	<i>View fax job queue / log</i>	<i>Modify fax send job</i>	<i>Cancel fax send job</i>
Fax send	Job owner	(note 2)			
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR			denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive		"Create" *	"Read"	"Modify"	"Delete"
	<i>Operation:</i>	<i>Create fax receive job</i>	<i>View fax receive status / log</i>	<i>Modify fax receive job</i>	<i>Cancel fax receive job</i>
Fax receive	Fax owner	(note 3)		denied	denied
	U.ADMIN(a)	(note 4)		denied	denied

	"Create" *	"Read"	"Modify"	"Delete"
U.NORMAL(a)	(note 4)	denied	denied	denied
U.ACCOUNTMANAGER	(note 4)	denied	denied	denied
U.FAXOPERATOR	(note 4)		denied	denied
U.ADDRESSBOOKOPERATOR	(note 4)	denied	denied	denied
Unauthenticated	(note 4)	denied	denied	denied

Application note:

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

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

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

Note 3: Job Owner of received faxes is assigned by default or configuration. Ownership of received faxes is assigned to U.FAXOPERATOR and U.ADMIN role.

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

6.4.2. FDP_ACF.1 Security attribute based access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in **Table 12** and **Table 13**.

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 12 and Table 13**.

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

6.4.3. FDP_FXS_EXT.1 Extended: Fax separation

(for O.FAX_NET_SEPARATION)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.4.4. 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 [*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.

6.5. Class FIA: Identification and Authentication

6.5.1. FIA_AFL.1 Authentication failure handling

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within [1 - 30]*] unsuccessful authentication attempts occur related to [*the unsuccessful user authentication attempts of following the last successful authentication or clear of user account lock*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*lockout each account in lockout time, U.ADMIN(a) and U.ACCOUNTMANAGER can release a lockout account*].

6.5.2. FIA_ATD.1 User attribute definition

(for O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*User ID, Role*].

6.5.3. FIA_PMG_EXT 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: [*“!””, “@”, “#”, “\$”, “^”, “*”, “(”, “)””, [refer to Table 14]*];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*none*].

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

6.6. Class FMT: Security Management

6.6.1. FMT_MOF.1 Management of security functions behavior

(for O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable, enable*] the functions [*Secure Channel*] to *U.ADMIN(a)*.

6.6.2. FMT_MSA.1 Management of security attributes

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control,

~~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 [*query, modify, delete, [create, export]*] the security attributes [*User ID, Role*] to [See *Table 15*].

Table 15 Security Attributes List

Security Attributes	Operation	User
User ID	<i>create, modify, query, delete, export</i>	<i>U.ADMIN(a)</i>
	<i>query, export</i>	<i>U.ACCOUNTMANAGER</i>
	<i>query</i>	<i>U.NORMAL, U.ADDRESSBOOKOPERATOR</i>
User ID (Except for U.ADMIN(a))	<i>create, modify, delete</i>	<i>U.ACCOUNTMANAGER</i>
Role	<i>create, modify, query, delete, export</i>	<i>U.ADMIN(a)</i>
	<i>query, export</i>	<i>U.ACCOUNTMANAGER</i>
	<i>query</i>	<i>U.NORMAL, U.ADDRESSBOOKOPERATOR</i>
Role (Except for U.ADMIN(a))	<i>create, modify, delete</i>	<i>U.ACCOUNTMANAGER</i>

6.6.3. FMT_MSA.3 Static attribute initialization

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

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

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

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

6.6.4. FMT_MTD.1 Management of TSF data

(for O.ACCESS CONTROL)

Hierarchical to: No other components.

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

FMT_MTD.1.1 Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 16.**

Table 16 Management of TSF Data

Data	Operation	Authorised role(s)
User Password of <i>U.NORMAL</i>	<i>modify</i>	<i>the owning U.NORMAL</i>
	<i>modify, export</i>	<i>U.ADMIN(a)</i> <i>U.ACCOUNTMANAGER</i>
User Password of <i>U.ADMIN(a)</i>	<i>modify, export</i>	<i>U.ADMIN(a)</i>
User Password of <i>U.ACCOUNTMANAGER</i>	<i>modify, export</i>	<i>U.ADMIN(a),</i> <i>U.ACCOUNTMANAGER</i>
User Password of <i>U.ADDRESSBOOKOPERATOR</i>	<i>modify</i>	<i>the owning</i> <i>U.ADDRESSBOOKOPERATOR</i>
	<i>modify, export</i>	<i>U.ADMIN(a),</i> <i>U.ACCOUNTMANGER</i>
Allowable Number of entry for Login Password	<i>modify</i>	<i>U.ADMIN(a)</i>
Lockout Time	<i>modify</i>	<i>U.ADMIN(a)</i>
Locked-out Account Status	<i>clear</i>	<i>U.ADMIN(a),</i> <i>U.ACCOUNTMANGER</i>
Auto Logout Time	<i>modify</i>	<i>U.ADMIN(a)</i>
Date and Time Information	<i>modify</i>	<i>U.ADMIN(a)</i>
Minimum Password Length	<i>modify</i>	<i>U.ADMIN(a)</i>
Address Book	<i>create,</i> <i>modify,</i> <i>delete</i>	<i>U.ADMIN(a),</i> <i>U.ADDRESSBOOKOPERATOR</i>
SYSLOG Server Settings	<i>modify</i>	<i>U.ADMIN(a)</i>
FTP Server Settings	<i>modify</i>	<i>U.ADMIN(a)</i>
Software	<i>query,</i> <i>modify</i>	<i>U.ADMIN(a)</i>

6.6.5. FMT_SMF.1 Specification of Management Functions

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions:
[refer to **Table 17**].

Table 17 Management Functions

SFR	Management	Management Functions	Reason
FAU_GEN.1	There are no management activities foreseen.	None	-
FAU_GEN.2	There are no management activities foreseen.	None	-
FAU_STG_EXT.1	The TSF shall have the ability to configure the cryptographic functionality.	None	This function is not provided.
FCS_CKM.1(b)	There are no management activities foreseen.	None	-
FCS_CKM.4(a)	There are no management activities foreseen.	None	-
FCS_CKM.4(b)	There are no management activities foreseen.	None	-
FCS_CKM_EXT.4	There are no management activities foreseen.	None	-
FCS_COP.1(b)	There are no management activities foreseen.	None	-
FCS_COP.1(c)	There are no management activities foreseen.	None	-
FCS_COP.1(f)	There are no management activities foreseen.	None	-
FCS_COP.1(g)	There are no management activities foreseen.	None	-
FCS_COP.1(h)	There are no management activities foreseen.	None	-
FCS_RBG_EXT.1(a)	There are no management activities foreseen.	None	-
FCS_RBG_EXT.1(b)	There are no management activities foreseen.	None	-
FCS_TLS_EXT.1	There are no management activities foreseen.	None	-
FCS_HTTPS_EXT.1	There are no management activities foreseen.	None	-
FCS_KDF_EXT.1(b)	There are no management activities foreseen.	None	-
FCS_KYC_EXT.1	There are no management activities foreseen.	None	-

SFR	Management	Management Functions	Reason
FDP_ACC.1	There are no management activities foreseen.	None	-
FDP_ACF.1	a) Management of attributes used for decision based on explicit access or denial.	None	The default value of an attribute is fixed and cannot be changed.
FDP_FXS_EXT.1	There are no management activities foreseen.	None	-
FDP_DSK_EXT.1	There are no management activities foreseen.	None	-
FIA_AFL.1	a) Management of the threshold for unsuccessful authentication attempts	Management of unsuccessful user authentication processing	-
	b) Management of actions which are taken for the unsuccessful authentication events	None	It is a predefined action and not managed.
FIA_ATD.1	a) If “assigned”, an authorized administrator can define additional security attributes to a user.	None	This function is not provided.
FIA_PMG_EXT.1	There are no management activities foreseen.	Minimum Password Length management	-
FIA_UAU.1	a) Authentication data management by an administrator	<ul style="list-style-type: none"> •Management of User Password (U.ACCOUNTMANAGER/U.ADMIN(a) /U.NORMAL /U.ADDRESSBOOKOPERATOR) by U.ADMIN(a). •Management of User Password (U.ACCOUNTMANAGER/U.NORMAL/U.ADDRESSBOOKOPERATOR) by U.ACCOUNTMANAGER 	-

SFR	Management	Management Functions	Reason
	b) Authentication data management by a relative user	<ul style="list-style-type: none"> • Management of own User Password by U.NORMAL • Management of own User Password by U.ADDRESSBOOKOPERATOR 	-
	c) List of actions to be taken before user authentication shall be managed.	None	It is a predefined action and not managed.
FIA_UAU.7	There are no management activities foreseen.	None	-
FIA_UID.1	a) Management of User Identity	Management of User ID	-
	b) If an authorized administrator can change the authorized actions before identification, the action list must be controlled.	None	It is a predefined action and not managed.
FIA_USB.1	a) An authorized administrator can define security attributes for a default subject.	None	There are no permitted roles.
	b) An authorized administrator can change security attributes of a subject.	None	There are no permitted roles.
FMT_MOF.1	a) Groups of roles which may affect reciprocally with the TSF Functions shall be managed.	None	It is a predefined action and not managed.
FMT_MSA.1	a) Groups of roles which may affect reciprocally with the Security Attributes shall be managed.	None	It is a predefined action and not managed.
	b) Rules for which the Security Attributes take over any particular values shall be managed.	None	It is a predefined action and not managed.
FMT_MSA.3	a) Groups which may be able to identify the default value shall be managed.	None	There are no roles to specify the default value.
	b) Restrictive or permissive settings of the default value for the prescribed access control SFP shall be managed.	None	The default value is fixed and cannot be changed.

SFR	Management	Management Functions	Reason
	c) Rules for which the Security Attributes take over any particular values shall be managed.	None	The rules cannot be changed.
FMT_MTD.1	a) Groups of roles which may affect reciprocally with the TSF Data shall be managed.	None	It is a predefined action and not managed.
FMT_SMF.1	There are no management activities foreseen.	None	-
FMT_SMR.1	a) Management of Groups of Users who are part of the Role.	None	It is a predefined action and not managed.
FPT_SKP_EXT.1	There are no management activities foreseen.	None	-
FPT_STM.1	a) Management of time	Management of the time stamp settings	-
FPT_TST_EXT.1	There are no management activities foreseen.	None	-
FPT_TUD_EXT.1	There are no management activities foreseen.	Management of the Software	-
FTA_SSL.3	a) Specification of the time in which an user who may cause termination of the interactive session between each user is non-active	None	Users cannot configure the setting individually.
	b) Specification of the default time in which an user who may cause termination of the interactive session is non-active	Specification of the default time in which a user is non-active after a session finishes.	-
FTP_ITC.1	a) Configuration of actions which require the trusted channel, if supported.	Secure channel settings	-
FTP_TRP.1(a)	a) Configuration of actions which require the trusted path, if supported.	None	It is a predefined action and not managed.
FTP_TRP.1(b)	a) Configuration of actions which require the trusted path, if supported.	None	It is a predefined action and not managed.
-	-	<ul style="list-style-type: none"> •Address Book management •SYSLOG Server Settings •FTP Server Settings 	-

6.6.6. FMT_SMR.1 Security roles

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles *U.ADMIN(a)*, *U.ACCOUNTMANAGER*, *U.ADDRESSBOOKOPERATOR*, and *U.NORMAL*

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

6.7. Class FPT: Protection of the TSF

6.7.1. 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.

6.7.2. FPT_STM.1 Reliable time stamps

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.7.3. 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.

6.7.4. 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 [*no other functions*] prior to installing those updates.

6.7.5. 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**.

6.8. Class FTA: TOE Access

6.8.1. FTA_SSL.3 TSF-initiated termination

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*refer to Table 18*].

Table 18 Time Interval of User Inactivity

Interface	Auto Logout Time
Control Panel	15 - 150 Sec.
Web Browser	5 - 999 Min.
Printer Driver	There is no inactive sessions

6.9. Class FTP: Trusted Paths/Channels

6.9.1. 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 [TLS]** to provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [SYSLOG server, Ftp server, mail server]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2 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 [*SYSLOG service, FTP service, mail service*].

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

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or

FCS_TLS_EXT.1 Extended: TLS selected, or
 FCS_SSH_EXT.1 Extended: SSH selected, or
 FCS_HTTPS_EXT.1 Extended: HTTPS selected].

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

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

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

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

(for O.COMMS_PROTECTION))

Hierarchical to: No other components.

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

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

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

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

6.10. Security Assurance Requirements

Table 19 lists the security assurance requirements for the Protection Profile for Hardcopy Devices – v1.0. ASE_SPD.1 is added to the component set defined in EAL1 of the evaluation assurance level in this table.

Table 19 TOE Security Assurance Requirements

Assurance Class	Assurance Component	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

Assurance Class	Assurance Component	Assurance Components Description
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Assurance Class	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

6.11. Security Functional Requirements Rationale

6.11.1. Dependencies of Security Functional Requirements Documents

Table 20 shows the analysis results of dependencies for the TOE Security Functional Requirements in this ST.

Table 20 Analysis Results of Dependencies for Security Functional Requirements

TOE Security Functional Requirements	Dependencies Required by CC and PP	Fulfilled Dependencies in ST	Un-fulfilled Dependencies in ST	Reason
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None	
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1	None	
FAU_STG_EXT.1	FAU_GEN.1, FTP_ITC.1	FAU_GEN.1, FTP_ITC.1	None	
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	None	
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(g), FCS_CKM_EXT.4, FCS_RBG_EXT.1(a), FCS_RBG_EXT.1(b)	None	
FCS_CKM.4(a)	[FCS_CKM.1(a), or FCS_CKM.1(b)]	FCS_CKM.1(a), FCS_CKM.1(b)	None	
FCS_CKM.4(b)	[FCS_CKM.1(a), or FCS_CKM.1(b)]	FCS_CKM.1(a), FCS_CKM.1(b)	None	
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(a), FCS_CKM.4(b)	None	
FCS_COP.1(a)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	None	
FCS_COP.1(b)	[FCS_CKM.1(a)], FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	None	
FCS_COP.1(c)	None	None	None	

TOE Security Functional Requirements	Dependencies Required by CC and PP	Fulfilled Dependencies in ST	Un-fulfilled Dependencies in ST	Reason
FCS_COP.1(f)	FCS_CKM.1(b), FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	None	
FCS_COP.1(g)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	None	
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	None	
FCS_SMC_EXT.1	FCS_COP.1(c)	FCS_COP.1(C)	None	
FCS_RBG_EXT.1(a)	None	None	None	
FCS_RBG_EXT.1(b)	None	None	None	
FCS_TLS_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	FCS_CKM.1(a), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1(b)	None	
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1	None	
FPT_KYP_EXT.1	None	None	None	
FCS_KYC_EXT.1	[FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(i), FCS_KDF_EXT.1, and/or FCS_COP.1(f)]	FCS_KDF_EXT.1, FCS_SMC_EXT.1, FCS_COP.1(f)		
FCS_KDF_EXT.1	FCS_COP.1(h)	FCS_COP.1(h)	None	
FDP_DSK_EXT.1	FCS_COP.1(d)	None	FCS_COP.1(d)	A self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP is used.
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None	
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	None	
FDP_FXS_EXT.1	None	None	None	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	None	
FIA_ATD.1	None	None	None	
FIA_PMG_EXT.1	None	None	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.1	None	
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	None	

TOE Security Functional Requirements	Dependencies Required by CC and PP	Fulfilled Dependencies in ST	Un-fulfilled Dependencies in ST	Reason
FIA_UID.1	None	None	None	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	None	
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None	
FMT_MSA.1	[FDP_ACC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1	None	
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	None	
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None	
FMT_SMF.1	None	None	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.1	None	
FPT_SKP_EXT.1	None	None	None	
FPT_STM.1	None	None	None	
FPT_TST_EXT.1	None	None	None	
FPT_TUD_EXT.1	FCS_COP.1(b), FCS_COP.1(c)	FCS_COP.1(b), FCS_COP.1(c)	None	
FTA_SSL.3	None	None	None	
FTP_ITC.1	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	None	
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	None	
FTP_TRP.1(b)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	None	

6.11.2. Security Assurance Requirements Rationale

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

7. TOE Summary Specification

Summary Specification of the TOE Security Functionality (TSF) is described in this Chapter.

7.1. Audit

The Summary Specification of the Class FAU Requirements is described as follows.

FAU_GEN.1

The TOE generates audit logs and record them in the audit log file when audit-relevant events occur. This causes FAU_GEN.1 to be realized.

Table 21 Recorded Events and Audit Logs

Auditable events	Events	Recorded User ID	Result
Start-up of audit functions	MFP power-on	None	None
Shutdown of audit functions	MFP power-off	None	None
Job completion	Print job completion	Job owner	Success or failure
	Scan job completion	Job owner	Success or failure
	Copy job completion	Job owner	Success or failure
	Fax transmission job completion	Job owner	Success or failure
	Fax reception job completion	Job owner	Success or deletion
Unsuccessful user authentication and identification	Failure of login	Logged in User	Success or failure
Unsuccessful user identification	Failure of login (Print Job)	User not registered in the TOE	Failure
Use of management functions	Addition of User	User who made modifications	Success or failure
	Change of User ID	User who made modifications	Success or failure
	Deletion of User	User who made modifications	Success
	Change of the settings	User who made modifications	Success
Modification to the group of Users that are part of a role	Change of the role information	User who made modifications	Success
Changes to the time	Modification of the time	User who made modifications	Success
Failure to establish session	Failure of TLS session establishment	None	Success or failure

The TOE adds the following data to the events to be audited.

- Date and Time: Time when an error/event occurred.
- Message: Sentence which describes the event content (Reason of failure when session failed)
- Error Code: An event is defined as a code, and represented as 4-digit hexadecimal numbers.
- User ID: Identifier of a Logged in user
- Result: Result of event implementation

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings, Power key
- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

FAU_GEN.2

If an auditable event occurs, the TOE realizes FAU_GEN.2 by attaching the user ID of a user who caused the event to the audit log.

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings, Power key
- TopAccess: Login, Job status, Registration, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

FAU_STG_EXT.1

U.ADMIN(a) can set the SYSLOG server as the server where an audit log is transferred from the Admin settings in TopAccess.

The TOE can save the generated audit log to the internal storage device first, then transfer the data to the SYSLOG server which is the external audit log server using the communication protocol TLS1.2. The maximum number of records which can be stored in the storage area of the audio log in the internal storage is as follows: 10,000 message logs, 5,000 print logs, 5,000 scan logs, 5,000 Fax transmission journals, and 5,000 Fax reception journals. When the maximum number of records of each log reaches the limit, the oldest audit data will be deleted to save the newest one.

Only U.ADMIN(a) can refer to all the audit logs which were saved to the internal storage and other users can refer to own job log only by access control.

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings, Power key
- TopAccess: Login, Job status, Registration, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

7.2. Cryptographic Support

The following describes the summary specifications for requirements of Class FCS.

FCS_CKM.1(a)

The TOE creates the RSA key pair as the asymmetric cryptographic key used for server certificate for TLS communication by the rsakpg1-crt method described in Section 6.3.1.3. of NIST SP 800-56B, Revision 1. Random numbers used for key creation is created by CTR_DRBG (AES-256) according to FCS_RBG_EXT.1(b). The Server certificate and server private key, including the generated public key is saved to the self-encrypting drive after being encrypted. The TOE does not include the TOE-specific extensions, unique processing which is not written in HCD-PP, or another implementation which is permitted, for the TSF.

The following shows the TSFI related to this requirement.

[Relevant TSFI]

- TopAccess: Admin settings

FCS_CKM.1(b)

The TSF creates a session key and HMAC key for communication at the TLS communication negotiation. The session key and HMAC key are created from the random number shared between the server and client. The random number is created by CTR_DRBG (AES-256) according to FCS_RBG_EXT.1(b). The parameters of each key differ depending on the selected Cipher Suite as shown below.

● Session key

A session key is used for encrypting the communication data. The used cryptographic algorithm and key length differ depending on the selected Cipher Suite. The cryptographic algorithm uses AES-CBC, and 128bit and 256bit can be selected as the session key length.

● HMAC key

A HMAC key is used to verify the pseudo random function (PRF) and communication data for key extension. The key for key extension generates the 256-bit MAC key and the key for data verification generates the MAC key with the key length according to Cipher Suite.

These keys are saved to the volatile memory and deleted by turning off the power.

[Relevant TSFI]

- Conform to TSFI of FTP_ITC_EXT.1, FTP_TRP.1(a) and FTP_TRP.1(b)

The TSF generates a key derivation key by Hash_DRBG (SHA-512) according to FCS_RBG_EXT.1(a) before switching to the TOE settings. At this time, the TSF derives the host authentication key 256bit used for the self-encrypting drive to authenticate the MFP according to FCS_KDF_EXT.1 and FCS_SMC_EXT.1 based on the key derivation key. A challenge code used for protecting the host authentication key is generated by a random number which was generated by the random number generation function of the self-encrypting drive (JCMVP authentication No.: F0022).

[Relevant TSFI]

- Control Panel: Power key (Only for the first start-up after TOE establishment)
Others: Main switch (Only for the first start-up after TOE establishment)

FCS_CKM_EXT.4/FCS_CKM.4(a)

The following keys and BEV handled by the TSF are discarded when they became unnecessary.

- Host authentication key for self-encrypting drive

This key is handled as a unnecessary key when the MFP is disposed. It is discarded by overwriting the area where the key is stored with a random number using Hash_DRBG (SHA-512) by a random number generator according to FCS_RBG_EXT.1(a).

The TSFI related to this requirement is as shown below.

[Relevant TSFI]

- Control Panel: Power key (At the first start-up after HDD initialization)
- Others: Main switch (At the first start-up after HDD initialization)

- Key derivation key, intermediate key (output value of FCS_KDF_EXT.1), host authentication key, challenge code, response code, session key and HMAC key for communication.

They are saved to the volatile memory and deleted by turn off the power.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FCS_CKM_EXT.4/FCS_CKM.4(b)

The following keys handled by the TSF are discarded when they are unnecessary.

- Secret key of the server

The secret key of the server is stored in the nonvolatile storage of the self-encrypting drive by being encrypted. It is handled as an unnecessary key when the administrator generates a new certificate during operation, and the area where the key is stored is overwritten three times with a fixed value. The key stored in the volatile memory is deleted by turning off the power.

The TSFI related to this requirement is as shown below.

[Relevant TSFI]

- TopAccess: Admin settings
- Control Panel: Power key
- Others: Main switch

FCS_COP.1(a)

The TSF encrypts and decrypts the communication data by operating the 128 bit or 256 bit cryptographic key generated by FCS_CKM.1(b) and AES cryptographic algorithm conforms to FIPS PUB197 in the CBC mode complies with NIST SP 800-38A so as to protect the communication data in FTP_ITC.1, FTP_TRP.1(a), and FTP_TRP.1(b).

The TSFI related to this requirement is as shown below.

[Relevant TSFI]

- Conform to TSFI of FTP_ITC.1, FTP_TRP.1(a), and FTP_TRP.1(b)

FCS_COP.1(b)

The TSF uses the RSA digital signature algorithm (rDSA) of which the key length is 2048bit which complies with the Digital Signature Standard prescribed in FIPS PUB 186-4 for creation of signatures during device certificate creation and verification of the server certificate by FTP_ITC.1

and firmware update by FPT_TUD_EXT.1. The TSF uses RSASSA-PKCS1-v1_5 for creation of the signatures during device certificate creation and verification of the server certificate, and RSASSA-PSS for verification of firmware update. Also, the RSA key generated by FCS_CKM.1 (a) is used for creation of the certificate.

The TSFI related to this requirement is as shown below.

[Relevant TSFI]

- Conform to TSFI of FCS_ITC.1 and FPT_TUD_EXT.1.
- TopAccess: Admin settings

FCS_RBG_EXT.1(a)

The TSF generates a random number using entropy source and DRBG when generating and destroying the host authentication key for storage encryption of TOE. This DRBG uses Hash_DRBG (SHA-512) to generate random numbers according to NIST SP 800-90A. The entropy source includes a hardware-based noise source, and outputs an entropy input which has at least 128-bit entropy and Nonce which has 64-bit entropy from the entropy source to DRBG according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”. The noise source uses the ES of the hardware embedded in SoC (Intel Atom Processor E3825) of the TOE. Output from the noise source is used for seeding the DRBG in SoC, and outputted by the RDRAND instruction after processing according to CTR_DRBG (AES) of NIST SP 800-90A. It is known that the noise source includes the minimum entropy, 0.5bit or more per 1bit, by the description in [Rambus 2012], the RDRAND instruction is the output of the DRBG with the security strength of 128 bits which was initialized at the seed of 256 bit entropy from the noise source. The RDRAND instruction is reseeded from the ES after outputting 511 of 128 bits. Thus, the rngd daemon process which constitutes the entropy source collects the RDRAND instruction output of which the seed differs per 16 bytes by compressing $128 \times 512 = 65,536 \text{ bit} = 8,192 \text{ byte}$ acquired by the RDRAND instruction into 16 bytes by the AES-CBC-MAC processing, and temporarily compiles almost full entropy data in the three 2,500-byte buffers of rngd. The necessary entropy is sufficiently supplied from rngd to Linux PRNG. So the 32 byte data read from the /dev/random output of Linux PRNG by the TSF is supposed to be almost full entropy. Of the 128 bytes, 96 bytes are used as Entropy Input and Nonce, and are supplied as a seed value for Hash_DRBG(SHA-512). From the Minimum entropy estimate in Section 6 of NIST SP800-90B, the TSF developer confirmed that the /dev/urandom output included the minimum entropy, 5.7 bits or more per 8 bits, within the TOE operation conditions range. It is supposed that the 128 byte bit string of the /dev/urandom output includes the $729.6 (= 128 \times 8 \times 5.7 / 8)$ bit entropy even if it is not estimated as full entropy.

FCS_RGB_EXT.1 (a) is realized by making this bit string as the Entropy Input and supplying the seed value to Hash_DRBG (SHA-512).

[Relevant TSFI]

- Control Panel: Power key (Only for the first start-up after TOE establishment)
- Others: Main switch (Only for the first start-up after TOE establishment)

FCS_RBG_EXT.1(b)

The TSF generates a random number using an entropy source and DRBG to protect the communication data of FTP_ITC, FTP_TRP(a) and FTP_TRP(b) at the time of server key generation for TLS communication and negotiation of TLS communication. The DRBG generates a random number using CTR_DRBG (AES) according to NIST SP 800-90A. This CTR_DRBG (AES) uses the Entropy Input and Nonce as the seed materials to use the derivation function. The entropy source includes a hardware-based noise source, and outputs an entropy input which has at least 128-bit

entropy and Nonce which has 64-bit entropy from the entropy source to DRBG according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”. The noise source uses the ES of the hardware embedded in SoC (Intel Atom Processor E3825) of the TOE. Output from the noise source is used for seeding the DRBG in SoC, and outputted by the RDRAND instruction after processing according to CTR_DRBG (AES) of NIST SP 800-90A. It is known that the noise source includes the minimum entropy, 0.5bit or more per 1bit, by the description in [Rambus 2012], the RDRAND instruction is the output of the DRBG with the security strength of 128 bits which was initialized at the seed of 256 bit entropy from the noise source. The RDRAND instruction is reseeded from the ES after outputting 511 of 128 bits. Thus, the rngd daemon process which constitutes the entropy source collects the RDRAND instruction output of which the seed differs per 16 bytes by compressing $128 \times 512 = 65,536 \text{ bit} = 8,192 \text{ byte}$ acquired by the RDRAND instruction into 16 bytes by the AES-CBC-MAC processing, and temporarily compiles almost full entropy data in the three 2,500-byte buffers of rngd. The necessary entropy is sufficiently supplied from rngd to Linux PRNG. So the 32 byte data read from the /dev/random output of Linux PRNG by the TSF is supposed to be almost full entropy. From the Minimum entropy estimate in Section 6 of NIST SP800-90B, the TSF developer confirmed that the /dev/random output included the minimum entropy, 5.7 bits or more per 8 bits, within the TOE operation conditions range. Even if it is pessimistically estimated that it is not full entropy, it is estimated that the bit string of 32 bytes /dev/random output contains $182.4 (= 32 \times 8 \times 5.7 / 8)$ bits of entropy by the lower limit evaluation of the entropy amount according to Section 3.1.5 of NIST SP800-90B. Input this bit string to the OpenSSL random number which have a role equivalent to the conditioning component role in NIST SP800-90B, and output the two bit strings, 320 bit and 160 bit, of the OpenSSL random number from the entropy source respectively. From Section 3.1.5.2 and Section 6 of NIST SP800-90B, the output bit string of this conditioning component has at least 128 bit and 64 bit entropies. FCS_RGB_EXT.1 (b) is realized by making this bit string as the Entropy Input and Nonce, and supplying the seed value to CTR_DRBG (AES).

[Relevant TSFI]

- Conform to TSFI of FTP_ITC_EXT.1, FTP_TRP.1(a) and FTP_TRP.1(b)

7.3. Storage Encryption (Conditionally mandatory)

The following describes the summary specifications for the conditional requirements B.1.

FPT_KYP_EXT.1

The following keys constitute the key chain in FCS_KYC_EXT.1 of this TOE.

- Key derivation key
A key derivation key is a 256-bit random number generated by using Hash_DRBG (SHA-512) according to FCS_RBG_EXT.1, and saved to the volatile storage.
- Intermediate key (Output value of FCS_KDF_EXT.1)
An intermediate key is a 256-bit key derived from the key derivation key according to FCS_KDF_EXT.1, and saved to the volatile storage.
- Host authentication key
The value which XORed the 256-bit intermediate key (Output value of FCS_KDF_EXT.1) with the 256-bit value according to FCS_SMC_EXT.1 is used as the host authentication key. This host authentication key is saved to the volatile storage and the FROM. The FROM is a nonvolatile storage which is not field-replaceable.

- Challenge code

A challenge code is a 256-bit random number generated by using the random number generating function in the self-encryption drive, and saved to the volatile storage.

- Response code

A response code is an encrypted value used for encryption of the host authentication key by EAS-CBC according to FCS_COP.1(f) using the challenge code as the cryptographic key, and saved to the volatile storage.

FCS_KYC_EXT.1

- Host authentication key generation

An intermediate key is derived from the key derivation key according to FCS_KDF_EXT.1. The key derivation key is a 256-bit random number generated by using Hash_DRBG (SHA-512) according to FCS_RBG_EXT.1(a). The KDF processing prescribed in FCS_KDF_EXT.1 is performed for the key derivation key to derive the intermediate key. In FCS_COP.1(h), HMAC-SHA-512 is selected so that the security strength is maintained to be more than 256 bits. This random number was generated by giving a sufficient entropy amount (256 bits or more) to the DRBG.

Then, use the value which XORed the intermediate key with the 256-bit value according to FCS_SMC_EXT.1 as the host authentication key.

- Challenge response authentication

A challenge code is a 256-bit random number generated by using the random number generating function in the self-encrypting drive. This challenge code is transmitted to the system control board from the self-encrypting drive. In the system control board, the host authentication key is encrypted by AES-CBC according to FCS_COP.1(f) by making the challenge code as the cryptographic key. The encrypted value is sent to the self-encrypting drive from the system control board as the 256-bit response code. The BEV of the key chain in this TOE is this response code.

From the above, the security strength more than 256 bits is secured in each phase of the key chain.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FDP_DSK_EXT.1

The TSF encrypts the user data and confidential TSF data by saving them to the self-encrypting drive (JCMVP authentication No.: F0022). A host authentication key is saved to the MFP and self-encrypting drive when the MFP is configured as the TOE. This host authentication key is used so that the self-encrypting drive authenticates the system control board per power on. If authentication successfully finishes, data writing to the self-encrypting drive is enabled and the written data is automatically encrypted. There is no area which cannot be encrypted in the self-encrypting drive area used by the TOE. All the user data are encrypted and saved.

[Relevant TSFI]

- Conform to TSFI of FDP_ACC.1/FDP_ACF.1 and FMT_SMF.1.

7.4. Storage Encryption (Selective requirements)

The following describes the summary specifications for the requirements D.4 selected in Storage Encryption.

FCS_COP.1(f)

The TSF encrypts the random number which was generated by the random number generating function in the self-encrypting drive per power on (hereinafter, referred to as challenge code) by AES-CBC by making the host authentication key as the cryptographic key. The value in which the challenge code is encrypted is sent to the system control board from the self-encrypting drive of the TOE. The system control board encrypts the host authentication key by AES-CBC by using the challenge code as the key encryption key. The value in which the host authentication key is encrypted is sent to the self-encrypting drive from the system control board of the TOE.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FCS_KDF_EXT.1

The TSF derives the intermediate key by the method conforms to KDF in Counter Mode of NIST SP800-108 using the random number which was generated by the random number generator at Hash_DRBG (SHA-512) according to FCS_RBG_EXT.1(a) as a sub mask with the hash function with a key according to FCS_COP(h).1

[Relevant TSFI]

- Control Panel: Power key (Only for the first start-up after TOE establishment)
- Others: Main switch (Only for the first start-up after TOE establishment)

FCS_SMC_EXT.1

The TSF function outputs the value which XORed the intermediate key outputted by FCS_KDF_EXT.1 with the 256-bit value. This value is used as the host authentication key.

[Relevant TSFI]

- Control Panel: Power key (Only for the first start-up after TOE establishment)
- Others: Main switch (Only for the first start-up after TOE establishment)

FCS_COP.1(h)

The TSF uses HMAC-SHA-512 which conforms to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”, and ISO/IEC 10118 for calculating the hash message function with a key in FCS_KDF_EXT.1 during derivation of the intermediate key from the key derivation key. The HMAC key length is 256 bits, hash function is SHA-512, block length is 512 bits, and outputted MAC length is 512 bits.

[Relevant TSFI]

- Control Panel: Power key (Only for the first start-up after TOE establishment)
- Others: Main switch (Only for the first start-up after TOE establishment)

7.5. Communication Protection (Selective requirements)

The following describes the summary specifications for the selective requirements D.2.

FCS_TLS_EXT.1

The TSF supports the TLS communication for communication with each type of servers mentioned in FTP_ITC.1 and communication with the client PC mentioned in FTP_TRP.1(a)/FTP_TRP.1(b). The TLS communication supported by the TSF is TLS1.2 (RFC 5246).

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Communication between TSF and Client PC

- The TSF generates the server secret key and public key of the RSA used for the TLS communication according to FCS_RBG_EXT.1(b) and FCS_CKM.1(a). The signature of the server certificate is generated by using the secret key and hash algorithm according to FCS_COP.1(b) and FCS_COP.1(c).
- The following shows how to share the secret random number data.
 - The TSF decrypts the secret random number encrypted by the RSA public key which was sent from the client PC using the server secret key. The TSF generates the session key and HMAC key from the secret random number through the pseudo random function (PRF) using the hashing (HMAC) with a key for message authentication according to FCS_COP.1(c) and FCS_COP.1(g).
- The following shows how to encrypt and verify the communication data.
 - The TSF verifies alteration of the communication data by using the HMAC key according to FCS_COP.1(c) and FCS_COP.1(g).
 - The TSF encrypts and decrypts the communication data in the AES-CBC mode according to FCS_COP.1 (a).

[Relevant TSFI]

- Conform to TSFI of FTP_TRP.1(a) and FTP_TRP.1(b).

Communication between TSF and Servers

- The following shows how TSF verifies the digital signature of the server certificate sent from various servers.
 - TSF calculates the hash value for server certificate verification according to FCS_COP.1(c).
 - TSF decrypts the digital signature of the server certificate by RSA signature verification according to FCS_COP.1 (b), and verifies the tampering of the server certificate by comparing it with the hash value for server certificate verification described above.
- The following shows how to share the secret random number data.
 - The TSF generates a secret random number according to FCS_RBG_EXT.1(b) for generating the session key and HMAC key.

- The TSF encrypts the secret random number using the RSA server public key which was sent from each server. The TSF generates the session key and HMAC key from the secret random number through the pseudo random function using the hashing (HMAC) with a key for message authentication according to FCS_COP.1(c) and FCS_COP.1(g).
- The following shows how to encrypt and verify the communication data.
 - The TSF verifies alteration of the communication data by using the HMAC key according to FCS_COP.1(c) and FCS_COP.1(g).
 - The TSF encrypts and decrypts the communication data in the AES-CBC mode according to FCS_COP.1 (a).

[Relevant TSFI]

- Conform to TSFI of FTP_ITC.1.

Communication between TSF and Client PC using IPPS

- The TSF generates the server secret key and public key of the RSA used for the TLS communication according to FCS_RBG_EXT.1(b) and FCS_CKM.1(a). The signature of the server certificate is generated by using the secret key and hash algorithm according to FCS_COP.1(b) and FCS_COP.1(c).
- The TSF decrypts the secret random number encrypted by the RSA public key which was sent from the client PC using the server secret key. The TSF generates the session key and HMAC key from the secret random number through the pseudo random function using the hashing (HMAC) with a key for message authentication according to FCS_COP.1(c) and FCS_COP.1(g).
- The TSF verifies alteration of the communication data by using the HMAC key according to FCS_COP.1(c) and FCS_COP.1(g).
- The TSF encrypts and decrypts the communication data in the AES-CBC mode according to FCS_COP.1(a).

[Relevant TSFI]

- Printer Driver: Interface to a Print request

FCS_HTTPS_EXT.1

The HTTP protocol which complies with RFC2818 is implemented so as to establish the trusted communication path between the TOE and the remote users. FCS_HTTPS_EXT.1 is realized by enabling the HTTPS communication using the TLS protocol which is specified at FCS_TLS_EXT.1.

[Relevant TSFI]

- TopAccess: Login, Job status, Account, User management, Admin settings

FCS_COP.1(g)

The TSF is used for the pseudo random function (PRF) which is used for generating the session key and HMAC key from a secret random number during the TLS communication. The TSF is also used for verifying alteration of the communication data in TLS communication. The hash message with a key is authenticated according to HMAC-SHA-1 in which the message length and key length that satisfy FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code", and FIPSPUB 180-3, "Secure Hash Standard" are 160 bits and HMAC-SHA-1 in which the message length and key

length are 256 bits. The hash function used at this time conforms to FCS_COP.1(c). From the above, FCS_COP.1(g) is realized.

[Relevant TSFI]

- Conform to FTP_TRP.1(a), FTP_TRP.1(b) and FTP_ITC.1

7.6. Trusted Update (Selective requirements)

The following describes the summary specifications for the selective requirements D.3.

FCS_COP.1(c)

A digital signature must be attached to the firmware to verify the authenticity of the firmware during firmware update at FPT_TUD_EXT.1. The cryptographic hash function conforms to SHA-256 which complies with ISO/IEC 10118-3:2004. The TSF performs signature generation or verification of the server certificate for TLS communication according to FCS_TLS_EXT.1. The cryptographic hash function used in that case complies with SHA-1, SHA-256, SHA-384 or SHA-512 conforming to ISO/IEC 10118-3:2004. The TSF authenticates the hash message with a key according to FCS_COP.1(g) during verification of the communication data integrity. The cryptographic hash function which is used at that time conforms to SHA-1 and SHA-256 which comply with ISO/IEC 10118-3:2004. The TSF authenticates the hash message with a key according to FCS_COP.1(h) during generation of the host authentication key. The cryptographic hash function which is used at that time conforms to SHA-512 which comply with ISO/IEC 10118-3:2004.

From the above, FCS_COP.1(c) is realized.

[Relevant TSFI]

- Conform to FTP_TRP.1(a), FTP_TRP.1(b) and FTP_ITC.1

7.7. User Data Protection

The following describes the summary specifications for the requirements for Class FDP.

FDP_ACC.1/FDP_ACF.1

The TOE performs access control for the user document data and operation for the user document data. Access control for the user document data allows access only when the user ID linked to the document data matched the user ID of a user who has been identified and authenticated at login. The access control for the user document operation is performed according to the roles retained by the user as shown in **Table 12** and **Table 13**.

FCC_ACC.1 and FDP.AFC.1 are realized by the access control shown in the table below.

Table 22 Print Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners who implement printing of the documents. • Allow browse and output of the documents implemented by the Job Owner. • Deny modification of the documents implemented by the Job Owner. • Allow deletion of the documents implemented by the Job Owner.

User	Access Control Rules
U.ADMIN(a)	<ul style="list-style-type: none"> • Allow implementation of the documents to be printed. • Deny implementation of the print documents implemented by other users. • Deny modification of the print documents implemented by other users. • Allow deletion of the print documents stored by other users.
U.NORMAL(a)	<ul style="list-style-type: none"> • Allow implementation of the documents to be printed. • Deny implementation of the print documents implemented by other users. • Deny modification of the print documents implemented by other users. • Deny deletion of the print documents stored by other users.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Deny implementation of the documents to be printed. • Deny browse of all implemented print documents. • Deny modification of all implemented print documents. • Deny deletion of all stored print documents.
Unauthorized User	<ul style="list-style-type: none"> • Allow the print documents implemented by the identified U.ADMIN(a) and U.NORMAL(a). • Deny browse of all implemented print documents. • Deny modification of all implemented print documents. • Deny deletion of all stored print documents.

[Relevant TSFI]

- Control Panel: Print
- Printer Driver: Interface to a Print request

Table 23 Scan Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.NORMAL(a) as the Job owner who implements scanning of the document. • Allow browse of the images scanned by the Job Owner. • Allow modification and deletion of the image scanned by the Job Owner.
U.ADMIN(a)	<ul style="list-style-type: none"> • Allow implementation of the documents to be scanned. • Deny browse of the images scanned by other users. • Deny modification of the images scanned by all users. • Allow deletion of the images scanned by the U.ADMIN(a) and deny deletion of the images scanned by other users.
U.NORMAL(a)	<ul style="list-style-type: none"> • Allow implementation of the documents to be scanned. • Deny browse of the images scanned by other users. • Deny modification and deletion of the images scanned by all users.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Deny implementation of the documents to be scanned. • Deny browse of all scanned images. • Deny modification and deletion of the images scanned by all users.

User	Access Control Rules
Unauthorized User	<ul style="list-style-type: none"> • Deny implementation of the documents to be scanned. • Deny browse of all scanned images. • Deny modification and deletion of all scanned images.

[Relevant TSFI]

- Control Panel: Scan, Simple Scan

Table 24 Copy Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners who implement copying of the documents. • Allow output of the copied documents printed by the Job Owner. • Deny modification and deletion of images personally saved. • Allow deletion of images personally saved.
U.ADMIN(a)	<ul style="list-style-type: none"> • Allow implementation of the documents to be copied. • Deny browse of the images copied by the other users. • Deny modification of the images copied and saved by the other users. • Allow deletion of the images copied and saved by the other users.
U.NORMAL(a)	<ul style="list-style-type: none"> • Allow implementation of the documents to be copied. • Deny browse of the images copied by the other users. • Deny modification of the images copied and saved by the other users. • Deny deletion of the images copied and saved by the other users.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Deny implementation of the documents to be copied. • Deny browse of all copied images. • Deny modification of all copied and saved images. • Deny deletion of all copied and saved images.
Unauthorized User	<ul style="list-style-type: none"> • Deny implementation of the documents to be copied. • Deny browse of all copied images. • Deny modification of all copied and saved images. • Deny deletion of all copied and saved images.

[Relevant TSFI]

- Control Panel: Copy, Simple Copy, Job display and Log display

Table 25 Fax Transmission Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN(a), U.NORMAL(a) and U.FAXOPERATOR as the Job owners who implement fax transmission of the documents. • Allow browse of the images scanned by the Job Owner. • Allow modification of the images personally saved. • Allow deletion of the images personally saved.

User	Access Control Rules
U.ADMIN(a)	<ul style="list-style-type: none"> • Allow implementation of Fax transmission documents. • Deny browse of the images scanned by the other users. • Deny modification of the images saved by the other users. • Allow deletion of the images saved by the other users.
U.NORMAL(a) U.FAXOPERATOR	<ul style="list-style-type: none"> • Allow implementation of Fax transmission documents. • Deny browse of the images scanned by other users. • Deny modification of images saved by the other users. • Deny deletion of images saved by the other users.
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Deny implementation of Fax transmission documents. • Deny browse of all scanned images. • Deny modification of all saved images. • Deny deletion of all saved images.
Unauthorized User	<ul style="list-style-type: none"> • Deny implementation of Fax transmission documents. • Deny browse of all scanned images. • Deny modification of all saved images. • Deny deletion of all saved images.

[Relevant TSFI]

- Control Panel: Fax, Job display and Log display

Table 26 Fax Reception Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN and U.FAXOPERATOR as the Job owners who implement fax reception of the documents. • Allow browse and print of all Fax-received documents. • Deny modification of all Fax-received documents. • Allow deletion of all Fax-received documents.
U.ADMIN(a) U.FAXOPERATOR	<ul style="list-style-type: none"> • Allow all Fax receptions regardless of the user's operation. • Allow browse and print of all Fax-received documents. • Deny modification of all Fax-received documents. • Allow deletion of all Fax-received documents.
U.NORMAL(a) U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Allow all Fax receptions regardless of the user's operation. • Deny browse and print of all Fax-received images. • Deny modification of all Fax-received images. • Deny deletion of all Fax-received images.
Unauthorized User	<ul style="list-style-type: none"> • Allow all Fax receptions regardless of the user's operation. • Deny browse and print of all Fax-received images. • Deny modification of all Fax-received images. • Deny deletion of all Fax-received images.
None	<ul style="list-style-type: none"> • All Fax-received images are received from the outside of the TOE regardless of the user's operation.

[Relevant TSFI]

- Control Panel: Print
- Others: PSTN Fax Interface

Table 27 Print Access Control for D.USERJOB

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners of the jobs printed by themselves.
U.ADMIN(a)	<ul style="list-style-type: none"> • Allow creation of the print jobs. • Allow browse of all print jobs. • Deny modification of all print jobs. • Allow cancel of all print jobs.
U.NORMAL(a)	<ul style="list-style-type: none"> • Allow creation of the print jobs. • Allow browse of all print jobs. • Deny modification of all print jobs. • Allow cancel of own print jobs, but deny cancel of other users' print jobs.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Deny creation of the print jobs. • Allow browse of all print jobs. • Deny modification of all print jobs. • Deny cancel of all print jobs.
Unauthorized User	<ul style="list-style-type: none"> • Allow creation of the print jobs. • Deny browse of all print jobs. • Deny modification of all print jobs. • Deny cancel of all print jobs.

[Relevant TSFI]

- Control Panel: Print, Job display and Log display
- TopAccess: Job status
- Printer Driver: Interface to a Print request

Table 28 Scan Access Control for D.USERJOB

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners of the jobs scanned by themselves.
U.ADMIN(a)	<ul style="list-style-type: none"> • Allow creation of the scanned jobs. • Allow browse of all scanned jobs. • Deny modification of all scanned jobs. • Allow cancel of all scanned jobs.
U.NORMAL(a)	<ul style="list-style-type: none"> • Allow creation of the scanned jobs. • Allow browse of all scanned jobs. • Deny modification of all scanned jobs. • Allow cancel of own scanned jobs, but deny cancel of other users' scanned job.
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR U.FAXOPERATOR	<ul style="list-style-type: none"> • Deny creation of the scanned jobs. • Allow browse of all scanned jobs. • Deny modification of all scanned jobs. • Deny cancel of all scanned jobs.
Unauthorized User	<ul style="list-style-type: none"> • Deny creation of the scanned jobs. • Deny browse of all scanned jobs. • Deny modification of all scanned jobs. • Deny cancel of all scanned jobs.

[Relevant TSFI]

- Control Panel: Scan, Simple Scan, Job display and Log display
- TopAccess: Job status

Table 29 Copy Access Control for D.USERJOB

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners of the copy jobs executed by themselves.
U.ADMIN(a)	<ul style="list-style-type: none"> • Allow creation of the copy jobs. • Allow browse of all copy jobs. • Deny modification of all copy jobs. • Deny cancel of all copy jobs.
U.NORMAL(a)	<ul style="list-style-type: none"> • Allow creation of the copy jobs. • Allow browse of all copy jobs. • Deny modification of all copy jobs. • Allow cancel of own copy jobs, but deny cancel of other users' copy jobs.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Deny creation of the copy jobs. • Allow browse of all copy jobs. • Deny modification of all copy jobs. • Deny cancel of all copy jobs.
Unauthorized User	<ul style="list-style-type: none"> • Deny creation of the copy jobs. • Deny browse of all copy jobs. • Deny modification of all copy jobs. • Deny cancel of all copy jobs.

[Relevant TSFI]

- Control Panel: Copy, Simple Copy, Job display and Log display
- TopAccess: Job status

Table 30 Fax Transmission Access Control for D.USERJOB

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN(a), U.NORMAL(a), and U.FAXOPERATOR as the Job owners of the fax transmission jobs executed by themselves.
U.ADMIN(a)	<ul style="list-style-type: none"> • Allow creation of Fax transmission jobs. • Allow browse of all Fax transmission jobs. • Deny modification of all Fax transmission jobs. • Allow cancel of all Fax transmission jobs.
U.NORMAL(a)	<ul style="list-style-type: none"> • Allow creation of Fax transmission jobs. • Allow browse of all Fax transmission jobs. • Deny modification of all Fax transmission jobs. • Allow cancel of own Fax transmission jobs, but deny cancel of other users' Fax transmission jobs.
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Deny creation of Fax transmission jobs. • Allow browse of all Fax transmission jobs. • Deny modification of all Fax transmission jobs. • Deny cancel of all Fax transmission jobs.

User	Access Control Rules
U.FAXOPERATOR	<ul style="list-style-type: none"> • Allow creation of Fax transmission jobs. • Allow browse of all Fax transmission jobs. • Deny modification of all Fax transmission jobs. • Allow cancel of own Fax transmission jobs, but deny cancel of other users' Fax transmission jobs.
Unauthorized User	<ul style="list-style-type: none"> • Deny creation of Fax transmission jobs. • Deny browse of all Fax transmission jobs. • Deny browse of all Fax transmission logs. • Deny modification of all Fax transmission jobs. • Deny cancel of all Fax transmission jobs.

[Relevant TSFI]

- Control Panel: Fax transmission, Job display and Log display
- TopAccess: Job status

Table 31 Fax Reception Access Control for D.USER.JOB

User	Access Control Rules
Job Owner	<ul style="list-style-type: none"> • Assign U.ADMIN and U.FAXOPERATOR as the Job owners of the fax reception jobs executed by themselves.
U.ADMIN(a) U.FAXOPERATOR	<ul style="list-style-type: none"> • Allow creation of all Fax-received Jobs regardless of the user's operation. • Allow browse of all Fax-received Jobs. • Deny modification of all Fax-received Jobs. • Allow cancel of all Fax-received Jobs.
U.NORMAL(a) U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	<ul style="list-style-type: none"> • Allow creation of all Fax-received Jobs regardless of the user's operation. • Deny browse of all Fax-received Jobs. • Deny modification of all Fax-received Jobs. • Deny cancel of all Fax-received Jobs.
Unauthorized User	<ul style="list-style-type: none"> • Allow creation of all Fax-received jobs. • Deny browse of all Fax-received Jobs. • Deny modification of all Fax-received Jobs. • Deny cancel of all Fax-received Jobs.

[Relevant TSFI]

- Control Panel: Job display and Log display
- TopAccess: Job status
- Others: PSTN Fax Interface

7.8. PSTN Fax-Network Separation

The following describes the summary specifications for the conditional requirements B.2.

FDP_FXS_EXT.1

Fax transmission and reception are only the functions of the Fax modem.

The Fax interface of the TOE is used only for transmission and reception of the Fax document data with the external Fax machines, and is not used for other purposes.

The Fax interface of the TOE supports only ITU-T-compliant G3 as the transmission/reception protocol. Thus, only transmission and reception using the Fax protocol are accepted in communication between the TOE and PSTN. However, communication in which the negotiation with Phase B is not established does not move to the subsequent phase and fails in the communication error, so the TOE disconnects the communication line.

From the above, bridge connection between the PSTN and LAN is prohibited.

[Relevant TSFI]

- Others: PSTN Fax Interface

7.9. Identification and Authentication

The following describes the summary specifications for the requirements for Class FIA.

FIA_AFL.1

- When the number of failed authentication, counted from the last succeeded authentication or login after releasing the account lock reaches the number of times set by the U.ADMIN (1 to 30), the TOE locks out the applicable user ID for a certain period of time.
- The function which releases the locked-out state of a user is provided for the U.ADMIN and U.ACCOUNTMANAGER.

[Relevant TSFI]

- Control Panel: Login
- TopAccess: Login, Admin settings

FIA_ATD.1

- The TOE associates the user ID and role with a user as the security attributes and registers and maintains them.

[Relevant TSFI]

- TopAccess: User management

FIA_PMG_EXT.1

The TOE provides the function to investigate the user password at registration and change of the password. Any combination of the following characters is allowed as a password: Upper and lower case letters, numbers, punctuation marks (+, -, . / : ; = ? ¥ _ ` { | } ~ space), special characters (! @#\$%^ *()), and European special characters (characters with the German umlauts and French cedilla: See **Table 14** for details.). It is also possible to set the minimum number of digits for a password to more than 15 letters by the U.ADMIN(a).

[Relevant TSFI]

- Control Panel: Home screen, Login, Admin settings
- TopAccess: Login, Account

FIA_UAU.7

If a user enters a password on the control panel, the TOE displays “●” as dummy characters on the control panel instead of the entered characters. Similarly, in the case that a user enters a password from the web browser, alternative characters are displayed instead of the entered characters. The alternative characters depend on the browser used by the user.

[Relevant TSFI]

- Control Panel: Login
- TopAccess: Login

FIA_UAU.1/FIA_UID.1

The TOE requires identification and authentication of a user. Identification and authentication of a user are executed to the user account database. If the user ID and password do not match the credential data which is internally saved, login is denied and an input prompt is displayed again for the user. The user ID of a job owner is associated with a print job performed from the client PC through the printer driver. The TOE identifies the user ID upon reception of a print job, and stores the print job in the print hold queue.

Also, the TOE saves a fax-received job internally without performing identification and authentication of the job.

[Relevant TSFI]

- Control Panel: Login
- TopAccess: Login
- Print driver: Interface to a Print request
- Others: PSTN Fax Interface

FIA_USB.1

The TOE associates a user with the user ID and role if identification and authentication are successfully finished.

[Relevant TSFI]

- Control Panel: Login
- TopAccess: Login

7.10. Security Management

The following describes the summary specifications for the requirements for Class FMT.

FMT_MOF.1

The TOE provides the U.ADMIN(a) only with the function which switches the Enable/Disable settings for secure channel function.

[Relevant TSFI]

- Control Panel: Admin settings
- TopAccess: Admin settings

FMT_MSA.1

The TOE provides the U.ADMIN(a) with the following functions.

- Creation, change, inquiry, deletion, and export of all user IDs
- Creation, change, inquiry, deletion, and export of all roles

The TOE provides the U.ACCOUNTMANAGER with the following functions.

- Inquiry and export of all user IDs
- Creation, change, and deletion of the user IDs except for the U.ADMIN(a)
- Creation, change and deletion of the roles except for the U.ADMIN(a)

The TOE provides the U.NORMAL and U.ADDRESSBOOKOPERATOR with the following functions.

- Inquiry of own user ID
- Inquiry of own role

[Relevant TSFI]

- TopAccess: User management

FMT_MSA.3

When a new D.USER.DOC and D.USER.JOB are created, the TOE assigns the user ID of the user who created them as the initial value of the security attribute.

The TOE does not provide the function which overwrites the initial value of the user ID which is the security attribute when the D.USER.DOC and D.USER.JOB are created.

[Relevant TSFI]

- Control Panel: Copy, Simple Copy, Scan, Simple Scan, Fax transmission
- TopAccess: User management
- Printer Driver: Interface to a Print request

FMT_MTD.1

The TOE provides the U.ADMIN(a) with the following operation functions.

- Change and export of the user password for the U.ADMIN(a).
- Change and export of the user password for the U.ACCOUNTMANAGER.
- Change and export of the user password for the U.ADDRESSBOOKOPERATOR.
- Change and export of the user password for the U.NORMAL.
- Change of the Allowable Number of entry for Login Password.
- Change of the lockout time.
- Status clear for all locked-out accounts.
- Change of the auto logout time.
- Change of the date and time information.
- Change of the minimum password length.
- Creation, change, and deletion of the address book.
- Change of the SYSLOG server settings.
- Change of the FTP server settings.
- Software version check and update

The TOE provides the U.ACCOUNTMANAGER with the following operation functions.

- Change and export of the user password for the U.ACCOUNTMANAGER.
- Change and export of the user password for the U.ADDRESSBOOKOPERATOR.
- Change and export of the user password for the U.NORMAL.
- Status clear for the locked-out accounts other than the U.ADMIN(a).

The TOE provides the U.NORMAL with the following operation functions.

- Change of the own user password.

The TOE provides the U.ADDRESSBOOKOPERATOR with the following operation functions.

- Change of the own user password.

[Relevant TSFI]

- Control Panel: Login, Home screen, Job display and Log display, Admin settings
- TopAccess: Login, Account, User management, Admin settings

FMT_SMF.1

The TOE provides the following security management functions to realize FMT_SMF.1.

Time Stamp Settings Management:

- Change operation of the date and time information by the U.ADMIN(a).

User ID Management:

- Change operation of the user ID by the U.ADMIN(a) or U.ACCOUNTMANAGER.

User Password Management:

- Change and export operation of the user password for U.ACCOUNTMANAGER, U.NORMAL, U.ADMIN(a) and U.ADDRESSBOOKOPERATOR by the U.ADMIN(a).
- Change and export operation of the user password for the U.ACCOUNTMANAGER, U.NORMAL, and U.ADDRESSBOOKOPERATOR by the U.ACCOUNTMANAGER.
- Change operation of the own user password by the U.NORMAL.
- Change operation of the user password by the U.ADDRESSBOOKOPERATOR.

Unsuccessful User Authentication Processing Management:

- Change operation of the number of entries of the login password by the U.ADMIN(a).
- Change operation of the lockout time by the U.ADMIN(a).
- Locked-out account status clear operation by the U.ADMIN(a) or U.ACCOUNTMANAGER.

Minimum Password Length Management:

- Change operation of the minimum password length by the U.ADMIN(a).

Specification of the inactive predetermined time for the user after the session is finished:

- Change operation of the auto logout time by the U.ADMIN(a).

Secure Channel Settings:

- Change operation of the Enable/Disable settings for TLS communication by the U.ADMIN(a).

Address Book Management:

- Change operation of the Address Book by the U.ADMIN(a).

SYSLOG Server:

- Change operation of the SYSLOG server settings by the U.ADMIN(a).

FTP Server:

- Change operation of the FTP server settings by the U.ADMIN(a).

Software:

- Software version confirmation and update by U.ADMIN(a).

[Relevant TSFI]

- Control Panel: Login, Home screen, Job display and Log display, Admin settings
- TopAccess: Login, Account, User management, Admin settings

FMT_SMR.1

The TOE retains a role related to the U.ADMIN(a), U.ACCOUNTMANAGER, U.NORMAL, and U.ADDRESSBOOKOPERATOR, and associates the role with the applicable user when a user is registered.

[Relevant TSFI]

- TopAccess: User management

7.11. Protection of the TSF

The following describes the summary specifications for the requirements for Class FPT.

FPT_SKP_EXT.1

- The TSF stores the encrypted server secret key in the self-encrypting drive, but does not provide a function to access all users.
- The TSF saves the key derivation key, intermediate key, challenge code and response code to the volatile memory in the plain text, but does not provide a function to access all users. These CSP will be deleted by turning off the power.
- The TSF saves the host authentication key to the FROM in the plain text, but does not provide a function to access all users.
- The TSF saves the session key and HMAC key for the TLS communication to the volatile memory in the plain text, but does not provide a function to access all users. These common keys are deleted by turning off the power.

From the above, FPT_SKP_EXT.1 is realized.

FPT_STM.1

The TOE uses “Year”, “Month”, “Day”, “Hour”, “Minute”, and “Second”, which are provided by the real clock IC embedded in the TOE for registration of the audit log, as a stamp to realize FPT_STM.1.

[Relevant TSFI]

- Conform to relevant TSFI of FAU_GEN.1, FAU_GEN.2

FPT_TST_EXT.1

The TOE conducts the following self-tests at power on.

- Health test of the firmware
Software that controls the MFP (SYSTEM FIRMWARE and SYSTEM SOFTWARE) implements verification by the electronic signature system which uses RSA as the public key system and SHA-256 as the hash function. Firmware of the printer unit (ENGINE FIRMWARE), scanner unit (SCANNER FIRMWARE), and fax unit (FAX FIRMWARE) respectively calculates 16-bit checksum to verify whether firmware is legitimate.

- Health test of the entropy source

Software that controls the MFP (SYSTEM SOFTWARE) starts the rngd process at power on and gets 4096 bytes from /dev/random of Linux PRNG to perform self verification according to NIST SP 800-90B. rngd calls the RDRAND instruction several times by retrying tight loop because entropy is supplied to Linux PRNG at this time. The SYSTEM SOFTWARE outputs a log of the abnormal detection and terminates the rngd process upon detection of the continuous error (CF=0) 10 times during the call. If the constant monitoring of the process monitoring task detects the termination of the rngd process, Service Call is displayed on the panel, and the TOE stops operation. When the RDRAND instruction is called, the continuous health test is automatically performed by the Online Health Test (OHT) which is embedded in SoC so as to assure that the noise source inside the entropy source is not broken. The frequency of occurrence of the 6-type bit patterns which are from the 1-bit through 4-bit length to the raw output of the noise source, 256 bit, is counted in the test. If the frequency is within the appropriate range, it is recorded as acceptable. If not, it is recorded as rejected. The probability that the identically distributed random numbers are judged as failure is about 1%. On the other hand, it is known by the description in [Rambus 2012] that occurrence of fatal failures, such that the output patterns of the noise source are fixed to 0 or 1 or 0 and 1 appear alternately, are detected. The OHT retains the recent 256 histories. If the results are acceptable more than 129, the RDRAND instruction returns the value together with CF=1. If not, an error is returned by CF=0. Also, the Built in Self Test (BIST) embedded in SoC which is executed automatically at power on confirms that the OHT within SoC and CTR_DRBG work correctly by the known answer so as to verify that the OHT works correctly. If an abnormality is detected in the BIST, the RDRAND instruction always returns an error by CF=0.

If an abnormality is detected in the above health test, an error code appears on the control panel, the TOE stops startup, and a user cannot use the TOE. The software TSF implemented in the firmware has verified the integrity of the execution code by the health test of the firmware. The hardware TSF uses the hardware-based noise source in the entropy source. Failures are detected by the verification whether the raw output of the noise source in the entropy source is correct by executing the functions of the health test embedded in SoC during the health test of the entropy source.

From the above, it is substantial as a test which verifies that the TSF works correctly at power on.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FPT_TUD_EXT.1

The TSF provides the U.ADMIN(a) with the Admin settings screen on the Home screen of the control panel as an interface to confirm the current software version information of the TOE, and the Admin settings screen on the control panel and the admin settings screen in TopAccess as the interfaces to update software.

Also, the TSF provides the digital signature verification function which verifies the authenticity of software to be updated before starting update. The verification method is as follows: Compare the hash value which is decrypted from the digital signature provided in the files of each firmware to be updated (SYSTEM SOTWAER, SYSTEM FIRMWARE, ENGINE FIRMWARE, SCNNER FIRMARE, and FAX1 FIRMWARE) by RSASSA-PSS according to FCS_COP.1(b) and the hash value which is derived from each firmware to be updated by SHA-256 according to FCS_COP.1(c). If the values match, it can be verified that the firmware is correct.

[Relevant TSFI]

- Control Panel: Home screen, Admin settings
- TopAccess: Admin settings

7.12. TOE Access

The following describes the summary specifications for the requirements for Class FTA.

FTA_SSL.3

The TOE forcibly logs the user out if the user does not operate the control panel for a certain period of time. The time can be set from 15 through 150 seconds. Also, a session is forcibly terminated and a user is logged out when the user does not operate for a certain period of time after accessing the TOE through the web browser. The time can be set from 5 through 999 minutes. The TOE does not create an interactive session when submitting a print job from the printer driver, but ends the session immediately after processing a print request.

[Relevant TSFI]

- Control Panel: Login
- TopAccess: Login

7.13. Trusted Path/Channel

The following describes the summary specifications for the requirements for Class FTP.

FTP_ITC.1

The TOE starts communication using TLS1.2 to protect data during communication between each server. In the case that the TOE accesses the mail server, SYSLOG server, and FTP server through the trusted channel, start of the TLS communication is requested to each server.

[Relevant TSFI]

- Control Panel: Power key, Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Print, Fax transmission, Job display and Log display, Admin settings
- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

FTP_TRP.1(a), FTP_TRP.1(b)

The TSF provides the following functions in order to prevent the communication data from leakage and provide the trusted path which detects alteration of the communication data in the communication path among the TOE, remote administrators, and remote users.

Communication with the WEB page:

- Connection is made by the HTTPS network protocol so as to establish the trusted path from the client PC to the web page of the TOE.
- Communication starts only in the case that the connection is made by the HTTPS protocol when a remote administrator and remote user connect to the web page of the TOE from the client PC using the web browser.
- The first administrator authentication, user authentication, and all remote user actions from the client PC are executed only for connection using the HTTPS protocol.

Print from the client PC:

- For printing from the client PC using the printer driver, connection should be made by the TLS communication protocol for establishing the trusted path during connection to the TOE.

[Relevant TSFI]

- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request

Table 32 defines the TSFI related to this Chapter.

Table 32 Definition of TSFI

TSFI Name	Details
Control Panel	
Power key	An interface which starts up and shuts down the MFP by turning off and on the main switch.
Login	An interface which identifies and authenticates a user who accesses the MFP from the control panel.
Home Screen	An interface which changes the user password and confirms the TOE version.
Copy	An interface which copies a document.
Simple Copy	An interface which copies a document.
Scan	An interface which scans an original as the image data, and previews, deletes, replaces, and inserts the scanned image data, saves the data to the folder in the FTP server, and sends the data to the specified email address.
Simple Scan	An interface which scans an original as the image data, and previews and deletes the scanned image data, and sends the data to the specified email address as an attached file.
Print	An interface which prints an original which was sent from the client PC and stored in the hold queue of the MFP and fax-received data.
Fax Transmission	An interface which scans an original as the image data, and previews, deletes, replaces, and inserts the scanned image data, and performs Fax transmission.
Job Display and Log Display	An interface which operates the execution status of Print and Scan and the Address Book data.
Admin Settings	An interface by which the Admin performs Security operations, such as change of the Admin password and Address Book data operation.
TopAccess	
Login	An interface which identifies and authenticates a user who accesses the MFP from the client PC.
Job Status	An interface which operates the active print job and scan job.
Account	An interface which changes the own password and displays the set role information.
User Management	An interface which executes management related to a user, such as registration of the user information.
Admin Settings	An interface which performs the MFP settings, such as the Auto Clear setting, and MFP management, such as the password policy setting and import of the Address Book.
Printer Driver	
Interface to a Print Request	An interface which holds (saves) the print data from the client PC to the MFP.

TSFI Name	Details
Others	
PSTN Fax Interface	An interface which receives the Fax data from the external Fax machines.
Main Switch	An interface which turns on the MFP and starts log collection to use the TOE.

Appendix

This Appendix describes the definition of acronyms and reference documents.

Table 33 Definition of Acronyms

Abbreviation	Definition
AES	Advanced Encryption Standard
BEV	Border Encryption Value
CBC	Cipher Block Chaining
CC	Common Criteria
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
DRAM	Dynamic Random Access Memory
DRBG	Deterministic Random Bit Generator
EE	Encryption Engine
FDE	Full Drive Encryption
FIPS PUB	Federal Information Processing Standards Publication
FRAM	Ferroelectric Random Access Memory
FROM	Flash ROM
FTP	File Transfer Protocol
GCM	Galois Counter Mode
HCD	Hardcopy Device
HDD	Hard Disk Drive
HMAC	Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol over SSL
IPP	Internet Printing Protocol
IPPS	IPP over SSL
IT	Information Technology
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
LAN	Local Area Network
LCD	Liquid crystal display
LED	light emitting diode
MFP	Multifunction Peripheral
NCU	Network control unit
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
PC	Personal Computer
PP	Protection Profile
PSTN	Public Switched Telephone Network
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol

Abbreviation	Definition
Soc	System-on-a-chip
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

- Reference Documents

[Rambus 2012]

- Analysis of Intel's Ivy Bridge Digital Random Number Generator, Cryptography Research a division of Rambus, 2012.
- Available: <https://www.rambus.com/intel-ivy-bridge-random-number-generator/>.