SHARP

SHARP BP-30C25 fax option model with BP-FR10U

Security Target

Version 1.03

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

SHARP CORPORATION

Revision history

Date	Ver.	Revision	Approved	Author
2020-02-17	0.80	• Original Draft	Hamada	Nakagawa
2020-02-28	0.81	• Sections 1.4.1 / 1.4.4 / 6.2.5 / 6.2.13.1 / 7.3 / 7.12 / 8.1: Correction of errors	Hamada	Nakagawa
2020-05-20	0.82	• Sections 1.4.3 / 2.4 / 6.2.2 / 6.2.5 / 6.2.13.1 / 7.3 / 7.12 / 8.1: Correction of description	Hamada	Nakagawa
2020-07-10	1.00	• Cover / Sections 1.1 / 1.2: Revised ST reference and TOE reference • Sections 1.4 / 6.2.3 / 6.2.4 / 6.2.5 / 6.2.12 / 7.2 / 7.12: Correction of description	Hamada	Yamamoto
2020-08-07	1.01	• Sections1.2 / 1.4.3.1 / 7.4: Correction of errors	Hamada	Nakagawa
2020-10-14	1.02	• Section 1.2 / Chapter 5 / Section 6.2.3 : In response to the obserbation reports ASE001-01 / ASE002-01 / ASE003-01	Hamada	Nakagawa
2020-11-02	1.03	• Section 1.2 / Section 1.4.1 : In response to the obserbation report ASE004-01	Hamada	Nakagawa

Table of Contents

1 ST Introduction 6
1.1 ST Reference 6
1.2 TOE Reference 6
1.3 TOE Overview 6
1.3.1 TOE Type 6
1.3.2 TOE Usage 6
1.3.3 TOE Main Security Functions 7
1.3.4 Required hardware/software/firmware other than the TOE 7
1.4 TOE Description 8
1.4.1 Physical Configuration of the TOE 8
1.4.2 Guidance 9
1.4.3 Logical Configuration of the TOE 9
1.4.4 Protected Assets of the TOE 12
1.4.5 User of the TOE 12
2 Conformance Claims 13
2.1 CC Conformance Claim 13
2.2 PP Claim 13
2.3 Package Claim 13
2.4 Conformance Rationale 13
3 Security Problem Definition 14
3.1 Threats 14
3.2 Organisational Security Policies 14
3.3 Assumptions 14
4 Security Objectives 15
5 Extended Components Definition 16
5.1 FAU_STG_EXT Extended: External Audit Trail Storage 16
5.2 FCS_CKM_EXT Extended: Cryptographic Key Management 16
5.3 FCS_HTTPS_EXT Extended: HTTPS selected 17
5.4 FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining) 18
5.5 FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation) 18
5.6 FCS_TLS_EXT Extended: TLS selected 19
5.7 FDP_DSK_EXT Extended: Protection of Data on Disk 20
5.8 FIA_PMG_EXT Extended: Password Management 21
5.9 FPT_KYP_EXT Extended: Protection of Key and Key Material 21
5.10 FPT_SKP_EXT Extended: Protection of TSF Data 22
5.11 FPT_TST_EXT Extended: TSF Testing 23
5.12 FPT_TUD_EXT Extended: Trusted Update 23
6 Security Requirements 25
6.1 Notational Conventions 25
6.2 Security Functional Requirements 25
6.2.1 Required FAU Requirements 25
6.2.2 Required FCS Requirements 26
6.2.3 Required FDP Requirements 28
6.2.4 Required FIA Requirements 30

6.2.5 Required FMT Requirements....31
6.2.6 Required FPT Requirements....34
6.2.7 Required FTA Requirements....35
6.2.8 Required FTP Requirements....35
6.2.9 Conditionally Mandatory Requirements B1....36
6.2.10 Selection-based Requirements D1....36
6.2.11 Selection-based Requirements D2....37
6.2.12 Selection-based Requirements D3....38
6.2.13 Rationale for Security Functional Requirements....38
6.3 TOE Security Assurance Requirements....41
6.3.1 Class ASE: Security Target Evaluation....41
6.3.2 Class ADV: Development....41
6.3.3 Class AGD: Guidance Documents....41
6.3.4 Class ALC: Life-cycle Support....41
6.3.5 Class ATE: Tests....41
6.3.6 Class AVA: Vulnerability Assessment....41
6.3.7 Rationale for Security Assurance Requirements....41
7 TOE Summary Specification....42
7.1 Security Audit....42
7.2 Cryptographic Support....44
7.3 User Data Protection....46
7.4 Identification and Authentication....49
7.5 Security Management....51
7.6 Protection of the TSF....54
7.7 TOE Access....55
7.8 Trusted Path / Channel....56
7.9 Confidential Data on Field-Replaceable Nonvolatile Storage Devices 1....57
7.10 Confidential Data on Field-Replaceable Nonvolatile Storage Devices 2....57
7.11 Protected Communications....58
7.12 Trusted Update....59
8 Appendix....60
8.1 Terminology....60
8.2 Abbreviations....60

List of Table

Table 1.1: TOE Component....6
Table 1.2: Required hardware/software/firmware for using the TOE function....7
Table 1.3: Guidance constituting the TOE....9
Table 3.1: Threats....14
Table 3.2: Organisational Security Policies....14
Table 3.3: Assumptions....14
Table 4.1: Security Objectives for the Operational Environment....15
Table 6.1: Auditable Events the PP Requires....25
Table 6.2: Auditable Events this ST Provides....26
Table 6.3: D.USER.DOC Access Control SFP....29
Table 6.4: D.USER.JOB Access Control SFP....29
Table 6.5: List of Security attributes....31
Table 6.6: Management of TSF Data....32
Table 6.7: List of Management Functions Provided by the TSF (1)....33
Table 6.8: List of Management Functions Provided by the TSF (2)....33
Table 6.9: List of Management Functions Provided by the TSF (3)....34
Table 6.10: List of Management Functions Provided by the TSF (4)....34
Table 6.11: Security Functional Requirement Dependencies (1)....39
Table 6.12: Security Functional Requirement Dependencies (2)....40
Table 6.13: Security Functional Requirement Dependencies (3)....40
Table 7.1: Information Recorded in Audit Data....42
Table 7.2: TSF Interface Regarding FAU_GEN.1/FAU_GEN.2....43
Table 7.3: TSF Interface related to D.USER.DOC Access Control....47
Table 7.4: TSF Interface related to D.USER.JOB Access Control....48
Table 7.5: TSF interface related to FMT_MTD.1....52
Table 7.6: TSF interface related to FMT_SMF.1....53
Table 8.1: Definition of terms used in this ST....60
Table 8.2: Definition of abbreviations used in this ST....60

List of Figure

Figure 1: Usage environment of the TOE....7
Figure 2: Physical configuration of the TOE....8
Figure 3: Logical configuration of the TOE....10

1 ST Introduction

This document is Security Target (ST) that describes the security of Sharp products described in Section 1.2. These Sharp products are CC Evaluation Targets (TOE) that claim conformance to this ST based on the IT security International Standard (the Common Criteria, CC) identified in Section 2.1. See Sections 8.1 and 8.2 for terminology used in this ST. This ST claims conformance to the PP shown in Section 2.1.

This chapter presents ST reference, TOE reference, TOE overview and TOE description.

1.1 ST Reference

This section provides information needed to identify this Security Target (ST).

Title: SHARP BP-30C25 fax option model with BP-FR10U
Security Target

Version: 1.03

Publication Date: 2020-11-02

Author: Sharp Corporation

1.2 TOE Reference

This section provides information needed to identify the Target of Evaluation (TOE) claiming conformance to this ST.

The entire TOE is identified as follows.

Name: SHARP BP-30C25 fax option model with BP-FR10U

Version: 0110Uc00

The above TOE consists of the combination of main units and mandatory options shown in Table 1.1.

Table 1.1: TOE Component

Version	Model number of Main unit	Fax	Mandatory option
0110Uc00	BP-30C25	none	BP-FR10U

1.3 TOE Overview

1.3.1 TOE Type

This TOE is an IT product and a digital multifunction device (abbreviated as MFD) equipped not only with copy, printer and scanner function, but also with a function to store and retrieve documents (referred to as document filing function in this TOE).

1.3.2 TOE Usage

The TOE is connected to a local area network (LAN) and used in a network environment. In the network environment, it is assumed to be used by being connected to the client PC and server in the internal network protected from unauthorized access of the external network by the firewall.
In this use environment, the user can operate the TOE from the operation panel of the TOE or by communication from the client PC via the LAN.
The main uses of the TOE are as shown below.

- Copy and print scanned document data by scanning paper documents (Copy function)
- Send document data from the client PC and print it (Printer function)
- Scan paper documents and send the scanned document data to the client PC or FTP server (Scanner function)
- Store scanned document data by scanning paper documents or received document data from the outside in the TOE, then retrieve them and print or send them (Document filing function)
- Make various settings of the MFD from the operation panel
- Make various settings of the MFD from the Web browser on the client PC (Web page setting)

1.3.3 TOE Main Security Functions

The TOE accumulates document data in the TOE or sends and receives it to and from the IT device connected to the LAN. To protect these document data and secret system information stored in the TOE against unauthorized disclosure and alteration, the TOE has the following security functions.

- Identification and authentication function: A function of identifying and authenticating whether the person who intends to use the TOE is an authorized user of the TOE
- Access control function: A function to restrict access to data stored in the TOE
- Stored data encryption function: A function to encrypt data on a field-replaceable nonvolatile storage device in the TOE
- Network protection function: A function to protect communication paths when using LAN
- Security management function: A function to restrict operations on TSF data to only administrators
- Audit function: A function to log and audit events related to TOE usage and security
- Software verification function: A function to verify the authenticity of firmware before software update of the TOE
- Self-testing function: A function to verify normal operation of TSF at TOE start-up

1.3.4 Required hardware/software/firmware other than the TOE

The general usage environment of the TOE is shown in Figure 1.

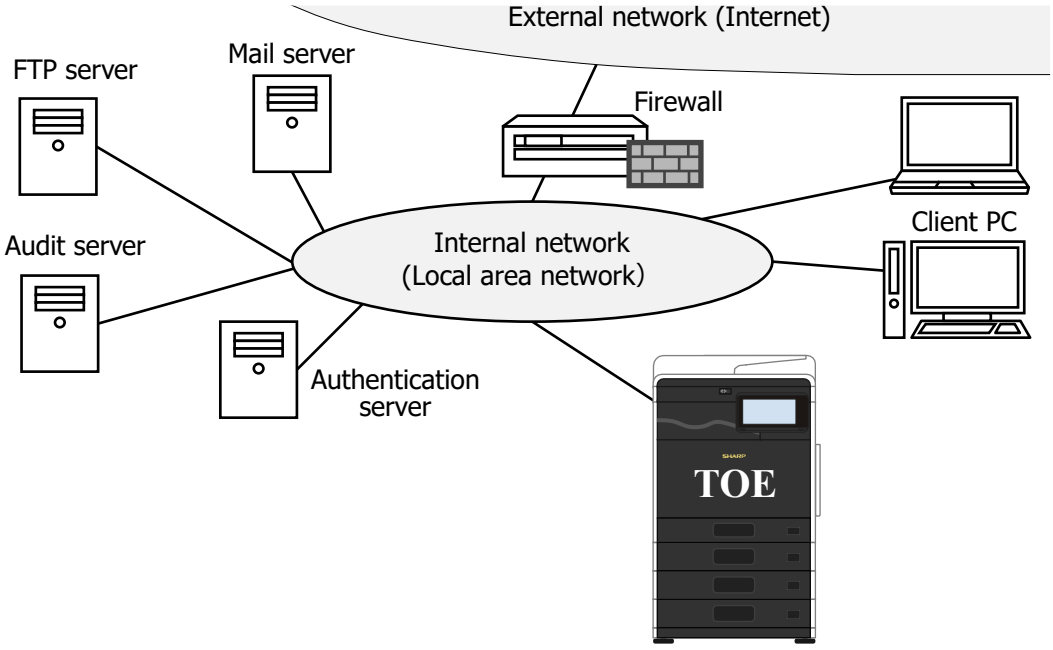

Figure 1: Usage environment of the TOE

The operation of the TOE requires at least a local area network and an audit server that supports TLS 1.2 using the syslog protocol. For the TOE evaluation, use an audit server configured with rsyslog.

The required hardware, software, or firmware for using the TOE function are shown in Table 1.2. In addition, various servers and web browsers must support TLS 1.2, and the printer driver needs to use the IPP-SSL function.

In addition, in order to connect the TOE to the external network, it is necessary to install a firewall to protect the TOE from unauthorized access of the external network.

Table 1.2: Required hardware/software/firmware for using the TOE function

TOE function	Required hardware / software / firmware	Configuration used in the TOE evaluation
Network authentication	Authentication server	openLDAP (2.4)
Web page setting	Client PC	Windows 10
	Web browser	Internet Explorer 11

Print from printer driver	Client PC	Windows 8.1
	Printer driver	SHARP BP-30C25 PCL6 driver
Scan to E-mail	Mail server	Postfix (2.10)
Scan to FTP	FTP server	Microsoft Internet Information Services installed on Windows 8.1

1.4 TOE Description

1.4.1 Physical Configuration of the TOE

The physical scope of the TOE is the entire MFD shown in Figure 2 and consists of the operation panel, scanner unit, engine unit, controller unit and internal storage. This is one in which the advanced security settings is enabled according to the instruction of the guidance, after installing the mandatory options for MFD main unit (BP-30C25 — Fax: none) shown in Table 1.1 and updating the firmware. It is possible to add a finisher or paper feed tray to the MFD, but they are not included in the TOE.

The operation panel, scanner unit, engine unit, controller unit (including CPU, Nonvolatile memory 1, NIC, ES, HBA, and Volatile memory) and internal storage are built in the MFD main unit and delivered from a dealer as the MFD.

The nonvolatile memory 2 is in the form of a board to be attached to the control unit in the MFD main unit and is provided as a part of an option product called Data Security Kit. Data Security Kit includes a USB memory that stores a binary data for update firmware in addition to the nonvolatile memory 2 and is delivered from a dealer as BP-FR10U.

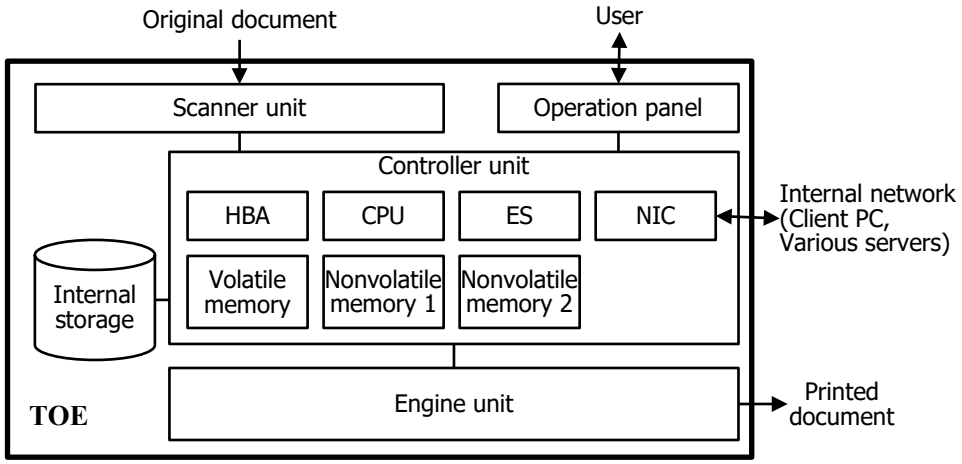

Figure 2: Physical configuration of the TOE

- Operation panel: A control device for operating the TOE equipped with touch panel LCD display, hardware key and LED.
- Scanner unit: A device for scanning paper documents and converting them into electronic data. Scanner control firmware for controlling the scanner operation is stored in the ROM in this device. The firmware is updated when the mandatory option BP-FR10U is installed.
- Engine unit: A device for printing and outputing paper documents, including the mechanism of paper feed function and paper output function. Print control firmware for controlling the print operation is stored in the ROM in this device. The firmware is updated when the mandatory option BP-FR10U is installed.
- Controller unit: A device for controlling the entire MFD, including such as integrated circuit, storage device for executing the firmware of the TOE shown below.
  - CPU: A central processing unit that performs basic arithmetic processing in MFD operation.
  - Volatile memory: A volatile storage device used as a work area.
  - NIC: A network interface device supporting Ethernet (10Base-T, 100Base-TX, 1000Base-T).
  - HBA (Host bus adapter): An interface device with cryptographic circuit to connect the controller unit and internal storage.

- ES (Entropy source): A circuit that generates random bit strings used to initialize a random number generator.
- Nonvolatile memory 1: A nonvolatile storage device that stores the main unit control firmware that performs Boot control of the MFD main unit and the key encryption key used for key encryption. This device is soldered on the board. The firmware is updated when the mandatory option BP-FR10U is installed.
- Nonvolatile memory 2: A nonvolatile storage device that stores the encryption key used for encrypting user data and TSF data on internal storage. The encryption key to be stored is key encrypted with the key encryption key stored in the nonvolatile memory 1. This device is installed by the mandatory option BP-FR10U.

● Internal storage: A field-replaceable nonvolatile storage device for storing user data such as document data, TSF data, and main control firmware for control of the MFD main unit. It consists of SSD and eMMC. The firmware is updated when the mandatory option BP-FR10U is installed.

1.4.2 Guidance

The list of guidance constituting the TOE is shown in Table 1.3.

Table 1.3: Guidance constituting the TOE

Name	Version	Language	Delivery format	Delivery method
Start Guide	TINSM2376QSZZ HH1	English	Paper medium	Enclosed in the package of the MFD main unit
Quick Start Manual	2020C-EX1	English	PDF file	Download or print from the MFD main unit
User's Manual	2020C-EX1	English	PDF file	Download or print from the MFD main unit
User's Manual (Touch Panel Operation)	2018H-EN1	English	PDF file	Download or print from the MFD main unit
User's Manual (Address Book Registration)	2018H-EN1	English	PDF file	Download or print from the MFD main unit
User's Manual (Web Page Settings)	2018H-EN1	English	PDF file	Download or print from the MFD main unit
Software Setup Guide	2020C-EN1	English	PDF file	Download or print from the MFD main unit
Troubleshooting	2020C-EN1	English	PDF file	Download or print from the MFD main unit
BP-FR10U Data Security Kit Operation Guide	EX1	English	PDF file	Stored in the CD-ROM enclosed in BP-FR10U
BP-FR10U Data Security Kit Notice	1.0	English	PDF file	Stored in the CD-ROM enclosed in BP-FR10U
How to set up BP-FR10U to be the "Protection Profile for Hardcopy Devices" compliant	V1.0	English	Paper medium	Enclosed in BP-FR10U

1.4.3 Logical Configuration of the TOE

Figure 3 shows the logical configuration of the TOE. The security function of the TOE is shaded.

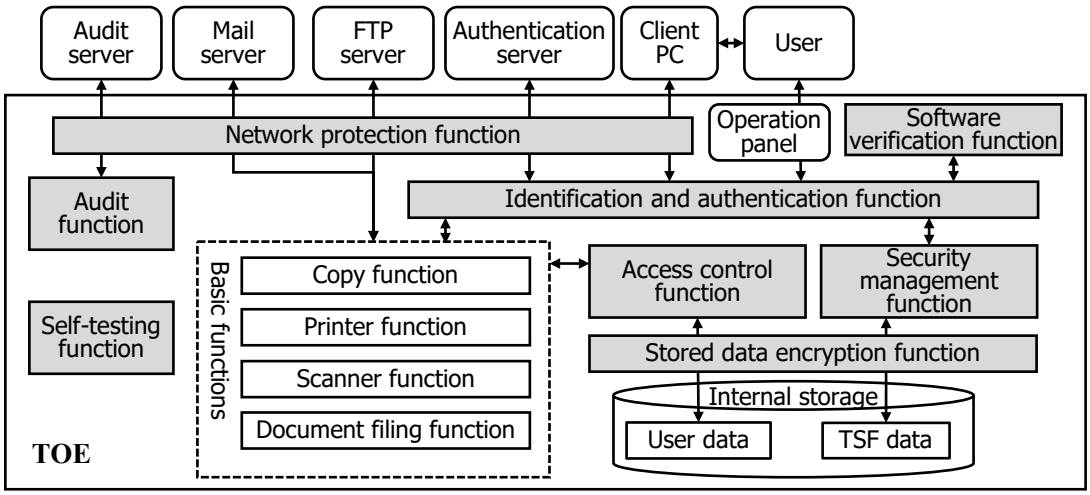

Figure 3: Logical configuration of the TOE

1.4.3.1 Basic function provided by the TOE

The TOE provides the following functions as basic functions.

- Copy function
  It is a function to copy and print document data scanned from paper documents by user's operation from the operation panel.
- Printer function
  It is a function to print document data received from the outside via LAN and a print function by printer driver.
  The print function by the printer driver is a function to receive the document data sent from the printer driver of the client PC and print it by user's operation from the operation panel.
- Scanner function
  It is a function to scan paper documents and send the scanned document data to the client PC or FTP server by user's operation from the operation panel.
  The transmission method is as shown below, and the user can transmit only to the E-mail address and FTP server registered in the address book in the TOE by the administrator.
  - E-mail transmission: Send to specified address as E-mail attachment
  - File server transmission: Send to specified FTP server
- Document filing function
  It is a function to store the document data in the internal storage and retrieve the stored data by user's operation from the operation panel or from the client PC via the LAN. It consists of the filing function, the scan to the local drive function and the retrieving function.
  The filing function is a function of simultaneously storing the document data to be printed or sent in the internal storage when the user uses the copy function, the printer function, or the scanner function.
  The scan to the local drive function is a function of storing document data scanned paper documents by user's operation from the operation panel in the internal storage. With this function only storing is done, printing and sending are not done.
  The retrieving function is a function that the user retrieves the document data stored in the internal storage and performs the operation described below.
  - Print: Printing document data on papers by user's operation from the operation panel.
  - Send: E-mail transmission, or file server transmission of document data is done by user's operation from the operation panel.
  - Preview: Displays the outline of the document data by the user's operation from the operation panel or from the client PC via the LAN.
  - Delete: Removes unnecessary document data from the internal storage by user's operation from the operation panel or from the client PC via the LAN.

1.4.3.2 Security function provided by the TOE

The TOE provides the following functions as security functions.

- Identification and authentication function
  A function to verify TOE's authorized user by login name and password and permit use of the TOE if it can be confirmed that it is authorized user of the TOE.
  The verification method includes internal authentication by user registration within the TOE and network authentication using an external authentication server.
  This function includes a function to display a password in dummy characters when entering a password from the operation panel. Furthermore, this function also includes a function to lock the authentication when the number of consecutive authentication failure times reaches the set value, a function to allow to register only the password that satisfies the conditions such as the minimum number of digits of the password preset by the administrator for protecting the quality of the password and a function to automatically log out when no operation state continues for a fixed time after login (identification and authentication).
- Access control function
  A function to restrict access to protected assets so that only authorized users can access protected assets within the TOE.
- Stored data encryption function
  A function to encrypt protected assets stored in internal storage to protect them from unauthorized access.
  This function also includes a function of generating an encryption key. Every time the TOE is started, the encryption key is generated by decrypting the key encrypted encryption key stored in the nonvolatile memory 2 using the key encryption key stored in the nonvolatile memory 1 and stored in the volatile memory.
- Network protection function
  A function to protect the communication path so as to prevent communication data flowing on the network when using the LAN from being leaked or altered by eavesdropping or the like.
  When communicating with the client PC, the audit server, the authentication server, the FTP server, and the mail server, it verifies the validity of the connection destination and protects the protected assets flowing over the network by encrypting them.
- Security management function
  A function to control that only the administrator of the TOE authenticated by the identification and authentication function can operate the TSF data shown below from the operation panel or the client PC via the LAN.
  - Register / delete internal authentication users
  - Change of user login name / password / authority group of internal authentication user (However, password can be changed by the user him- or herself)
  - Changing the minimum password length of user password
  - Change the identification and authentication method
  - Register / change / delete authority group
  - Change date / time
  - Query / change the audit log destination
  - Query / change the automatic logout time
  - Register / change / delete address book data
  - Register / change / delete available LDAP authentication servers
  - Change IP address settings
  - Query / Change mail transmission server settings
  - Update the firmware
- Audit function
  A function to record the log of events related to the use and security of the TOE with information such as date and time as audit log and provide the recorded audit log in auditable form.
  The recorded audit log is sent to the audit server using the network protection function and can be viewed from the audit server.
- Software verification function

A function to verify the authenticity of the update target firmware and confirm that it is legitimate, before starting TOE firmware update.

- Self-testing function
  A function to verify the TSF's normal operation by verifying the integrity of TSF execution code and TSF data at the time of TOE activation.

1.4.4 Protected Assets of the TOE

The protected assets covered by this TOE are classified as follows.

- D.USER (User Data)
  Data created by and for Users that do not affect the operation of the TSF
- D.TSF (TSF Data)
  Data created by and for the TOE that might affect the operation of the TSF

The above user data is composed of the following two types.

- D.USER.DOC (User Document Data)
  Information contained in a User’s Document, in electronic or hardcopy form
- D.USER.JOB (User Job Data)
  Information related to a User’s Document or Document Processing Job

The above TSF data is composed of the following two types.

- 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. The data handled by this TOE is as follows.
  - Internal authentication user login name, internal authentication user authority group, audit log, audit log destination settings, minimum password length, identification and authentication method, authority group, date / time, automatic logout time, address book, authentication server settings, IP Address settings, mail transmission server settings, scanner control firmware, print control firmware, main unit control firmware for performs Boot control of the MFD main unit, main control firmware for control of the MFD main unit
- 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. The data handled by this TOE is as follows.
  - Internal authentication user password, encryption key

1.4.5 User of the TOE

Users of this TOE (U.USER) are classified into authority groups as follows.

- U.NORMAL (Normal User)
  A User who has been identified and authenticated and does not have an administrative role.
- U.ADMIN (Administrator)
  A User who has been identified and authenticated and has an administrative role and access authority to all user data. Includes administrator (hereinafter referred to as "default administrator") account incorporated in the machine as factory default.

2 Conformance Claims

This ST satisfies the followings.

2.1 CC Conformance Claim

The CC versions to which this ST and TOE claim conformance and the compliance with CC Part 2 and Part 3 of this ST are as follows:

CC Conformance: Common Criteria version: Version 3.1, Release 5,
Part 2 (CCMB-2017-04-002) Extended, and
Part 3 (CCMB-2017-04-003) Conformant.

2.2 PP Claim

The PP to which this ST and TOE claim conformance is as follows:

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

In this ST, the above is simply referred to as PP unless otherwise noted.

2.3 Package Claim

This ST and TOE do not claim conformance to any package.

2.4 Conformance Rationale

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

- Required Uses
  - Printing, Scanning, Copying, Network communications, Administration
- Conditionally Mandatory Uses
  - Storage and retrieval, Field-Replaceable Nonvolatile Storage
- Optional Uses
  - (None)

3 Security Problem Definition

This chapter defines security problems of the TOE.

3.1 Threats

Threats to the TOE are described in Table 3.1.

Table 3.1: 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.

3.2 Organisational Security Policies

Organisational security policies are described in Table 3.2.

Table 3.2: Organisational 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	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.

3.3 Assumptions

Use and operation of the TOE requires the environment described in Table 3.3.

Table 3.3: 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

This chapter describes the measures to implement the security objective policies.

The security objectives for the operational environment are shown in Table 4.1.

Table 4.1: Security Objectives for the Operational Environment

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

5 Extended Components Definition

This ST defines the extended components as follows. These are a part of what is defined in PP.

- FAU_STG_EXT — External Audit Trail Storage
- FCS_CKM_EXT — Cryptographic Key Management
- FCS_HTTPS_EXT — HTTPS selected
- FCS_KYC_EXT — Cryptographic Operation (Key Chaining)
- FCS_RBG_EXT — Cryptographic Operation (Random Bit Generation)
- FCS_TLS_EXT — TLS selected
- FDP_DSK_EXT — Protection of Data on Disk
- FIA_PMG_EXT — Password Management
- FPT_KYP_EXT — Protection of Key and Key Material
- FPT_SKP_EXT — Protection of TSF Data
- FPT_TST_EXT — TSF Testing
- FPT_TUD_EXT — Trusted Update

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	1

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

Management:

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

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

Audit:

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

- There are no auditable events foreseen.

FAU_STG_EXT.1 Extended: Protected Audit Trail Storage

Hierarchical to: No other components.

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

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

Rationale:

The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

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

5.2 FCS_CKM_EXT Extended: Cryptographic Key Management

Family Behavior:

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

Component leveling:

FCS_CKM_EXT.4: Cryptographic Key Material Destruction	4

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Hierarchical to: No other components.

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

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

Rationale:

Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.

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

5.3 FCS_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	1

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: FCS_TLS_EXT.1 Extended: TLS selected

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_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.1: Key Chaining	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_KYC_EXT.1 Extended: Key Chaining

Hierarchical to: No other components.

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

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

Rationale:

Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain. However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.

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

5.5 FCS_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	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Rationale:

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

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

5.6 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: 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: 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 [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.

5.7 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: Protection of Data on Disk	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

Hierarchical to: No other components.

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

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

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

Rationale:

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

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

5.8 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	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FIA_PMG _EXT.1 Extended: Password management

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: *"!"*, *"@"*, *"#"*, *"$"*, *"%"*, *"^"*, *"&"*, *"*"*, *"("*, *")"*, [assignment: *other characters*]];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater.

Rationale:

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

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

5.9 FPT_KYP_EXT Extended: Protection of Key and Key Material

Family Behavior:

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

Component leveling:

FPT_ KYP_EXT.1: Protection of key and key material	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_ KYP _EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ KYP _EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device, 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.

5.10 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	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

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

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

5.11 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	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_TST_EXT.1 Extended: TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

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

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

5.12 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	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update

Hierarchical to: No other components.

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

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

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

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

Rationale:

Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.

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

6 Security Requirements

This chapter describes the security requirements.

6.1 Notational Conventions

- **Bold** typeface indicates the portion that has been completed or refined in PP.
- ***Bold italic*** typeface indicates the portion that has been “assignment”, “selection” or “refinement” in this ST. The value that has been "assignment" is shown in bracket [] of non-italic typeface, the value that has been "selection" is shown in bracket *[]* of italic typeface.
- For "iteration" by PP, component name, component label and element label followed by a lower case alphabet in parentheses, e.g., (a), (b)... represent unique identifier.
- *Italic* typeface indicates the portion that has been only used to emphasize description regardless of requirement operations.

6.2 Security Functional Requirements

This section describes the Security Functional Requirements (SFR) that the TOE should satisfy, based on the classification of PP.

6.2.1 Required FAU Requirements

This section describes functional requirements of FAU (Security Audit) class related to the required usage specified by PP.

FAU_GEN.1 Audit data generation (for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) **All auditable events specified in Table 6.1, [*and Table 6.2*]**.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 6.1, [*and Table 6.2*]**.

Table 6.1: Auditable Events the PP Requires

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

Note: User identification events and user authentication events are not separated and are considered as one event for audit purposes.

Table 6.2: Auditable Events this ST Provides

Auditable event	Relevant SFR	Additional information
Software update	FPT_TUD_EXT.1	Old and new version

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

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

FAU_STG_EXT.1 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.

6.2.2 Required FCS Requirements

This section describes functional requirements of FCS (Cryptographic Support) class related to the required usage specified by PP. The section 6.2.9, 6.2.10, 6.2.11 and 6.2.12 also describes a part of FCS requirements.

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

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(b) Cryptographic Operation (for signature generation/ verification)
FCS_COP.1(i) Cryptographic operation (Key Transport)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_CKM.1.1(a) **Refinement:** The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with *[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**.

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

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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

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

Hierarchical to: No other components.

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

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

FCS_CKM.4 Cryptographic key destruction (for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to: No other components.

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

FCS_CKM.4.1 **Refinement:** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- ***For volatile memory, the destruction shall be executed by [powering off a device, [single overwrite consisting of a pseudo-random pattern using the simple bit operation]].***
- ***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), 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]***.

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

Hierarchical to: No other components.

Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or~~ FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification) (for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation~~ FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(b) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a ***[***

- ***Digital Signature Algorithm (DSA) with key sizes (modulus) of*** [***2048 or 3072 bits***]
- ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of*** [***2048 or 3072 bits***]
- ***Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of*** [***256, 384, or 521 bits***]

] that meets the following ***[***

- ***FIPS PUB 186-4, "Digital Signature Standard"***
- ***The TSF shall implement "NIST curves" P-256, P384 and [P521] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***

].

FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) (for O.STORAGE_ENCRYPTION and O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from ***[[single] hardware-based noise source]*** 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.

6.2.3 Required FDP Requirements

This section describes functional requirements of FDP (User Data Protection) class related to the required usage specified by PP. The section 6.2.9, 6.2.10 and 6.2.11 also describes a part of FDP requirements.

FDP_ACC.1 Subset access control (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** on **subjects, objects, and operations among subjects and objects specified in Table 6.3 and Table 6.4**.

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 6.3 and Table 6.4**.

FDP_ACF.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 6.3 and Table 6.4**.

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***].

Table 6.3: D.USER.DOC Access Control SFP

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

Table 6.4: D.USER.JOB Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	*Operation:*	*Create print job*	*View print queue / log*	*Modify print job*	*Cancel print job*
	Job owner	(note 1)		***denied***	
	U.ADMIN			***denied***	
	U.NORMAL			denied	denied
	Unauthenticated	***denied***	***denied***	denied	denied
Scan	*Operation:*	*Create scan job*	*View scan status / log*	*Modify scan job*	*Cancel scan job*
	Job owner	(note 2)		***denied***	
	U.ADMIN			***denied***	
	U.NORMAL			denied	denied
	Unauthenticated	denied	***denied***	denied	denied
Copy	*Operation:*	*Create copy job*	*View copy status / log*	*Modify copy job*	*Cancel copy job*
	Job owner	(note 2)		***denied***	
	U.ADMIN			***denied***	
	U.NORMAL			denied	denied
	Unauthenticated	denied	***denied***	denied	denied
Storage / retrieval	*Operation:*	*Create storage / retrieval job*	*View storage / retrieval log*	*Modify storage / retrieval job*	*Cancel storage / retrieval job*
	Job owner	(note 1)		***denied***	
	U.ADMIN			***denied***	
	U.NORMAL			denied	denied
	Unauthenticated	***denied***	***denied***	denied	denied

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

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

6.2.4 Required FIA Requirements

This section describes functional requirements of FIA (Identification and Authentication) class related to the required usage specified by PP. The section 6.2.11 also describes a part of FIA requirements.

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 *[* [***3***] *]* unsuccessful authentication attempts occur related to [***the unsuccessful user (including administrator) internal authentication attempts following the last successful authentication***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *[* ***met*** *]*, the TSF shall [

- ***Unsuccessful authentication reached three times: Reception of authentication trials stops for five minutes***
- ***Five minutes later after stopping: the number of times authentication was unsuccessful is cleared, and the reception of authentication trials is recovered***

].

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 Login Name, Authority Groups***].

FIA_PMG_EXT.1 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: *[* ***"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"*** **[** ***no other characters*** **]** *]*;
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

FIA_UAU.1 Timing of authentication (for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 **Refinement:** The TSF shall allow [***nothing***] on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.7 Protected authentication feedback (for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [***substitute characters as many as ones that are provided***] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification (for O.USER_I&A and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 **Refinement:** The TSF shall allow [***nothing***] on behalf of the user to be performed before the user is identified.

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

FIA_USB.1 User-subject binding (for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [***User Login Name, Authority Groups***].

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: [***no rules***].

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: [***no rules***].

6.2.5 Required FMT Requirements

This section describes functional requirements of FMT (Security Management) class related to the required usage specified by PP.

FMT_MOF.1 Management of security functions behavior (for O.ADMIN_ROLES)

Hierarchical to: No other components.

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

FMT_MOF.1.1 **Refinement:** The TSF shall restrict the ability to *[**enable**]* the functions [
● ***Initialize Private Data / Data in Machine***
] to **U.ADMIN**.

FMT_MSA.1 Management of security attributes (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control~~, or FDP_IFC.1 Subset information flow control~~]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to *[**query**, **modify**, **delete**, [**create**]]* the security attributes [***Security attributes specified in Table 6.5***] to [***Authorised roles specified in Table 6.5***].

Table 6.5: List of Security attributes

Security attributes	Operation	Authorised roles
User Login Name of Internal Authentication User	***create, modify, delete***	**U.ADMIN**
Authority Groupe of Internal Authentication User	***create, modify, delete***	**U.ADMIN**
	query	**U.ADMIN, the owning U.NORMAL**

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.

FMT_MTD.1 Management of TSF data (for O.ACCESS_CONTROL)

Hierarchical to: No other components.

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

FMT_MTD.1.1 **Refinement:** The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 6.6**.

Table 6.6: Management of TSF Data

TSF Data	Operation	Authorised role(s)
Internal Authentication User Password	***create, delete***	**U.ADMIN**
	modify	**U.ADMIN, the owning U.NORMAL**
Minimum Password Length	***modify***	**U.ADMIN**
Identification and Authentication Method	***modify***	**U.ADMIN**
Date / Time	***modify***	**U.ADMIN**
Audit Log Destination Settings	***query, modify***	**U.ADMIN**
Automatic Logout Time	***query, modify***	**U.ADMIN**
Address Book	***create, modify, delete***	**U.ADMIN**
Authentication Server Settings	***create, modify, delete***	**U.ADMIN**
IP Address Settings	***modify***	**U.ADMIN**
Mail Transmission Server Settings	***query, modify***	**U.ADMIN**
Scanner Control Firmware	***modify***	**U.ADMIN**
Print Control Firmware	***modify***	**U.ADMIN**
Main Unit Control Firmware for Performs Boot Control of the MFD Main Unit	***modify***	**U.ADMIN**
Main Control Firmware for Control of the MFD Main Unit	***modify***	**U.ADMIN**

FMT_SMF.1 Specification of Management Functions (for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 **Refinement:** The TSF shall be capable of performing the following management functions: [***management functions specified in Table 6.7, Table 6.8, Table 6.9, and Table 6.10***].

Table 6.7: List of Management Functions Provided by the TSF (1)

SFR	Management functions	Notes
FAU_GEN.1	None	—
FAU_GEN.2	None	—
FAU_STG_EXT.1	• Configuration of audit log destination	Encryption function is fixed to use of TLS.
FCS_CKM.1(a)	None	—
FCS_CKM.1(b)	None	—
FCS_CKM_EXT.4	Initialization of private data and data in machine	—
FCS_CKM.4	Initialization of private data and data in machine	—
FCS_COP.1(a)	None	—
FCS_COP.1(b)	None	—
FCS_RBG_EXT.1	None	—
FDP_ACC.1	None	—
FDP_ACF.1	None	No rule for explicit permission / rejection.
FIA_AFL.1	None	Threshold value and action are fixed.
FIA_ATD.1	• Registration of internal authentication user • Change of internal authentication user authority group	—
FIA_PMG_EXT.1	• Change of minimum password length	—
FIA_UAU.1	• Change of identification and authentication method • Configuration of authentication server • Change of internal authentication user password	Action prior to authentication is fixed.
FIA_UAU.7	None	—
FIA_UID.1	• Change of identification and authentication method • Configuration of authentication server • Registration/deletion of internal authentication user • Change of internal authentication user login name	Action prior to identification is fixed.
FIA_USB.1	None	Subject attribute is fixed.

Table 6.8: List of Management Functions Provided by the TSF (2)

SFR	Management functions	Notes
FMT_MOF.1	None	Role group is fixed.
FMT_MSA.1	None	Role group and rule are fixed.
FMT_MSA.3	None	Role group, default settings and rule are fixed.
FMT_MTD.1	None	Role group is fixed.
FMT_SMF.1	None	—
FMT_SMR.1	• Management of authority group	—
FPT_SKP_EXT.1	None	—
FPT_STM.1	• Configuration of date / time	—
FPT_TST_EXT.1	None	—
FPT_TUD_EXT.1	• Update the firmware	—
FTA_SSL.3	• Configuration of automatic logout time	—
FTP_ITC.1	None	—
FTP_TRP.1(a)	None	—
FTP_TRP.1(b)	None	—

Table 6.9: List of Management Functions Provided by the TSF (3)

SFR	Management functions	Notes
FPT_KYP_EXT.1	None	—
FCS_KYC_EXT.1	None	—
FDP_DSK_EXT.1	None	—
FCS_COP.1(d)	None	—
FCS_COP.1(f)	None	—
FCS_TLS_EXT.1	None	—
FCS_HTTPS_EXT.1	None	—
FCS_COP.1(c)	None	—

Table 6.10: List of Management Functions Provided by the TSF (4)

SFR	Management functions	Notes
—	• Management of address book	—
—	• Configuration of IP address	—
—	• Configuration of mail transmission server	—

FMT_SMR.1 Security roles (for O.ACCESS_CONTROL. O.USER_AUTHORIZATION, and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

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

6.2.6 Required FPT Requirements

This section describes functional requirements of FPT (Protection of the TSF) class related to the required usage specified by PP. The section 6.2.9 also describes a part of FPT requirements.

FPT_SKP_EXT.1 Protection of TSF Data (for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_STM.1 Reliable time stamps (for O.AUDIT)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TST_EXT.1 TSF testing (for O.TSF_SELF_TEST)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TUD_EXT.1 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.

6.2.7 Required FTA Requirements

This section describes functional requirements of FTA (TOE Access) class related to the required usage specified by PP.

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 [***user inactivity for:***
- ***240 seconds or shorter, specified by U.ADMIN, for sessions via the operation panel***
- ***300 seconds, for sessions via web interfaces***

].

6.2.8 Required FTP Requirements

This section describes functional requirements of FTP (Trusted Paths / Channels) class related to the required usage specified by PP.

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:** ***[authentication server*****, [*** *audit log 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 [***authentication service, audit log service, ftp service, mail service***].

FTP_TRP.1(a) Trusted path (for Administrators) (for O.COMMS_PROTECTION)

Hierarchical to: No other components.

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

FTP_TRP.1.1(a) **Refinement:** The TSF shall **use** ***[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**.

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**.

6.2.9 Conditionally Mandatory Requirements B1

This section describes functional requirements related to Confidential Data on Field-Replaceable Nonvolatile Storage Devices among the conditionally mandatory usage specified by PP. The section 6.2.10 also describes a part of functional requirements for this section.

FPT_KYP_EXT.1 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**.

FCS_KYC_EXT.1 Key Chaining (for O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

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

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

FDP_DSK_EXT.1 Protection of Data on Disk (for O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

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

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

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

6.2.10 Selection-based Requirements D1

This section describes functional requirements related to Confidential Data on Field-Replaceable Nonvolatile Storage Devices among the selection-based requirements specified by PP. The section 6.2.9 also describes a part of functional requirements for this section.

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

Hierarchical to: No other components.

Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or~~
~~FDP_ITC.2 Import of user data with security attributes, or~~
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in *[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]***.

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]***.

6.2.11 Selection-based Requirements D2

This section describes functional requirements related to Protected Communications among the selection-based requirements specified by PP.

FCS_TLS_EXT.1 TLS selected (selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to: No other components.

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

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

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***
- ***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***

].

FCS_HTTPS_EXT.1 HTTPS selected (selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to: No other components.

Dependencies: FCS_TLS_EXT.1 Extended: TLS selected

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

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

FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) (selected with FCS_IPSEC_EXT.1.4)

Hierarchical to: No other components.

Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or~~
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material

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, SHA-384]*, key size [*160, 256, 384*], and message digest size *[160, 256, 384]* bit** that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**

6.2.12 Selection-based Requirements D3

This section describes functional requirements related to Trusted Update among the selection-based requirements specified by PP.

FCS_COP.1(c) Cryptographic operation (Hash Algorithm) (selected in FPT_TUD_EXT.1.3)

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**.

6.2.13 Rationale for Security Functional Requirements

As described above, the SFR claimed by this ST is a subset of the SFR specified by PP. All assignments and selections have been completed. Also, as described below, there is no problem with dependencies.

6.2.13.1 Rationale for Security Functional Requirement Dependencies

Table 6.11, Table 6.12, and Table 6.13 shows the dependencies that the SFRs specified by CC and PP should satisfy, the dependencies that this TOE satisfies, the dependencies that this TOE does not satisfy and the validity for this TOE not satisfying dependencies.

Table 6.11: Security Functional Requirement Dependencies (1)

Dependencies / Requirement	Stipulated	Satisfied	Unsatisfied	Remarks
FAU_GEN.1	FPT_STM.1	FPT_STM.1	—	—
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1	—	—
FAU_STG_EXT.1	FAU_GEN.1, FTP_ITC.1	FAU_GEN.1, FTP_ITC.1	—	—
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	—	—
FCS_CKM.1(b)	[FCS_COP.1(a), or FCS_COP.1(d), or FCS_COP.1(e), or FCS_COP.1(f), or FCS_COP.1(g), or FCS_COP.1(h)], FCS_CKM_EXT.4, FCS_RBG_EXT.1	FCS_COP.1(a), FCS_COP.1(d), FCS_COP.1(f), FCS_COP.1(g), FCS_CKM_EXT.4, FCS_RBG_EXT.1	—	—
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	—	—
FCS_CKM.4	[FCS_CKM.1(a) or FCS_CKM.1(b)]	FCS_CKM.1(a), FCS_CKM.1(b)	—	—
FCS_COP.1(a)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	—	—
FCS_COP.1(b)	[FCS_CKM.1(a)], FCS_CKM_EXT.4	FCS_CKM.1(a), FCS_CKM_EXT.4	—	—
FCS_RBG_EXT.1	—	—	—	—
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	—	—
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	—	—
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	—	—
FIA_ATD.1	—	—	—	—
FIA_PMG_EXT.1	—	—	—	—
FIA_UAU.1	FIA_UID.1	FIA_UID.1	—	—
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	—	—
FIA_UID.1	—	—	—	—
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	—	—

Table 6.12: Security Functional Requirement Dependencies (2)

Dependencies / Requirement	Stipulated	Satisfied	Unsatisfied	Remarks
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	—	—
FMT_MSA.1	[FDP_ACC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1	—	—
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	—	—
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1	FIA_UID.1	FIA_UID.1	—	—
FPT_SKP_EXT.1	—	—	—	—
FPT_STM.1	—	—	—	—
FPT_TST_EXT.1	—	—	—	—
FPT_TUD_EXT.1	FCS_COP.1(b), FCS_COP.1(c)	FCS_COP.1(b), FCS_COP.1(c)	—	—
FTA_SSL.3	—	—	—	—
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	—	—
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	—	—
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	—	—

Table 6.13: Security Functional Requirement Dependencies (3)

Dependencies / Requirement	Stipulated	Satisfied	Unsatisfied	Remarks
FPT_KYP_EXT.1	—	—	—	—
FCS_KYC_EXT.1	[FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(f), FCS_KDF_EXT.1, and/or FCS_COP.1(i)]	FCS_COP.1(f)	—	—
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	—	—
FCS_COP.1(d)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	—	—
FCS_COP.1(f)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	—	—
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	—	—
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1	—	—
FCS_COP.1(g)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	—	—
FCS_COP.1(c)	—	—	—	—

6.3 TOE Security Assurance Requirements

The security assurance requirement (SAR) claimed by this ST is shown below by the assurance class of CC Part 3. This ST uses the security assurance components defined in CC Part 3 and described in PP directly as SAR.

6.3.1 Class ASE: Security Target Evaluation

- Conformance claims: ASE_CCL.1 — Conformance claims
- Extended components definition: ASE_ECD.1 — Extended components definition
- ST introduction: ASE_INT.1 — ST introduction
- Security objectives: ASE_OBJ.1 — Security objectives for the operational environment
- Security requirements: ASE_REQ.1 — Stated security requirements
- Security problem definition ASE_SPD.1 — Security problem definition
- TOE summary specification ASE_TSS.1 — TOE summary specification

6.3.2 Class ADV: Development

- Functional Specification: ADV_FSP.1 — Basic functional specification

6.3.3 Class AGD: Guidance Documents

- Operational user guidance: AGD_OPE.1 — Operational user guidance
- Preparative procedures: AGD_PRE.1 — Preparative procedures

6.3.4 Class ALC: Life-cycle Support

- CM capabilities: ALC_CMC.1 — Labelling of the TOE
- CM scope: ALC_CMS.1 — TOE CM coverage

6.3.5 Class ATE: Tests

- Independent testing: ATE_IND.1 — Independent testing - conformance

6.3.6 Class AVA: Vulnerability Assessment

- Vulnerability analysis: AVA_VAN.1 — Vulnerability survey

6.3.7 Rationale for Security Assurance Requirements

The above SAR claimed by this ST is completely consistent with the SAR stipulated by PP.

7 TOE Summary Specification

This chapter indicates that the security functional requirements (SFR) are satisfied by describing a summary specification of the TOE security functions (TSF).

7.1 Security Audit

This section describes the summary specification on the required FAU requirements in Section 6.2.1.

FAU_GEN.1 / FAU_GEN.2

In addition to the start / end of the audit, the TSF generates audit event logs of audit events described in Table 6.1 and Table 6.2 as the audit data.
The TSF acquires the date (year / month / day) and time (hour / minute / second) on which the audit event including the start / end of the audit occurred from the system clock of the TOE and records it in the audit data.
The TSF records the user login name (the entire or head part of the login name) in the audit data as subject identification information related to the audit event for the event generated by a specific user. However, if the TOE itself generates an event, it will be recorded as "SYSTEM", if the subject can not be specified, it will be recorded as "N/A". Table 7.1 shows the information recorded by TSF in audit data.

Table 7.1: Information Recorded in Audit Data

Event Name	Date and Time *1	Operation I/F *2	Login Name	Results *3	Additional Information
Audit Start	Yes	N/A	N/A	Yes	N/A
Audit End	Yes	N/A	N/A	Yes	N/A
Job Completion	Yes	Yes	Job owner	Yes	Completed job name
I&A Failure	Yes	Yes	Character string entered as a login name	N/A	N/A
Add User	Yes	Yes	User who performed the addition	Yes	Added login name
Change Password	Yes	Yes	User who performed the change	Yes	Login name of the user whose password is changed.
Change Login Name	Yes	Yes	User who performed the change	Yes	Login name after change
Delete user	Yes	Yes	User who performed the deletion	Yes	Deleted login name (In the case of “All User Deletion”, “ALL”.)
Add Auth Group	Yes	Yes	User who performed the addition	Yes	Added authority group name
Change Role	Yes	Yes	User who performed the change	Yes	• Login name of the user whose authority group he belongs is changed • Authority group name after change
Change Auth Group Setting	Yes	Yes	User who performed the change	Yes	Authority group name of which setting is changed
Change Time Setting	Yes	Yes	User who performed the change	Yes	N/A
Change Setting	Yes	Yes	User who performed the change	Yes	• Setting item of which setting value is changed • Setting value after change
Comm Failure *The communication counterpart is the audit server	Yes	N/A	SYSTEM	N/A	Reason of failure

Comm Failure *The communication counterpart is except for the audit server	Yes	Net	N/A	N/A	• IP address of the starter of the communication • IP address of the communication counterpart • Communication direction • Reason of failure
Modify Addr Book	Yes	Yes	User who performed the modify	Yes	Add: Internal control ID and address name of the added entry Deletion/change: Internal control ID of the deleted/changed entry
Firm Update	Yes	Yes	User who performed the update	Yes	• Firmware name • Firmware version before update • Firmware version after update

*1 The event occurrence date and time is notated in the extended format of ISO 8601.
*2 Any of Ope / Web / Net is notated as an operation interface. However, "N/A" is described in the table, "N/A" is notated.
*3 Any of Success / Failure is notated as an event execution result. However, "N/A" is described in the table, "N/A" is notated.

The TSF interface related to this requirement is as shown in Table 7.2.

Table 7.2: TSF Interface Regarding FAU_GEN.1/FAU_GEN.2

Event Name	Interface
Audit Start	• Turn on the MFD power (Recovery from power failure is treated as equivalent)
Audit End	• Turn off the MFD power
Job Completion	• According to TSF interface of FDP_ACC.1/FDP_ACF.1, generate job from copy / printer / scanner / document filing function.
I&A Failure	• Login operation on user authentication screen of the operation panel or the web page.
Add User	• Add user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.
Change Password	• Modify user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.
Change Login Name	• Modify user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.
Delete User	• Delete user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.
Add Auth Group	• Add authority group from [User Control] →[Access Control Settings] →[Authority Group] in the settings mode of the operation panel or on the web page.
Change Role	• Modify user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.
Change Auth Group Setting	• Modify authority group from [User Control] →[Access Control Settings] →[Authority Group] in the settings mode of the operation panel or on the web page.
Change Time Setting	• Configure date and time from [System Settings]→[Common Settings] →[Device Control]→[Clock Adjust] in the settings mode of the operation panel or on the web page.
Change Setting	• Change setting value from various settings in the settings mode of the operation panel or on the web page.
Comm Failure	• Communicate with authentication server / audit server / FTP server / mail server, according to TSF interface of FTP_ITC.1.
Modify Address Book	• Add / edit / delete from [Address Book] on the operation panel. • Add / edit / delete from [Address Book]→[Address Book] on the web page.
Firm Update	• Move to the maintenance mode on the operation panel and update firmware.

FAU_STG_EXT.1

The generated audit data is sent to the audit server using the Syslog protocol and TLS 1.2 according to FTP_ITC.1. The data is stored in the buffer area prepared in the internal storage until the transmission succeeds. In this buffer area, it is possible to store 40,000 audit data. Transmission of audit data is performed at the timing when new data is generated.

When the transmission to the audit server fails, a warning message is displayed on the screen of the operation panel and the web page, and the transmission to the audit server is retried periodically until it succeeds. The warning message describes that it is not connected to the audit server and the impact of that and requires to inform the administrator.
When the usage rate of the buffer area reaches 80% or more, it is restricted that only the default administrator can login. This restriction is canceled when the usage rate of the buffer area becomes less than 70%. In the state where the buffer area is full, that is, when 40,000 audit data is stored in the buffer area, the newly generated audit data is not stored in the buffer area but is deleted.
Audit data stored in the buffer area is encrypted according to FDP_DSK_EXT.1 and stored. In addition, regardless of the authority group, all users can not access the audit data stored in the buffer area.
The TSF interface related to this requirement conforms to the TSF interface of FAU_GEN.1 / FAU_GEN.2.

7.2 Cryptographic Support

This section mainly describes the summary specification of the required FCS requirements in Section 6.2.2.

FCS_CKM.1(a)

The TSF generates the RSA key as the asymmetric key used for establishing the key of the encrypted communication by the rsakpg1-basic method described in 6.3.1.1 of the standard document NIST SP 800-56B Revision 1. Random numbers required at that time are generated according to FCS_RBG_EXT.1. With respect to this TSF, the TOE does not include the TOE specific extension, proprietary processing outside this standard, or another allowed implementation. This key is stored in the internal storage in a state encrypted with the storage key.

The TSF interface related to this requirement is as follows.

- Initial startup after TOE installation.
- Execute [Create] in [System Settings]→[Security Settings]→[Certificate Management]→[Device Certificate Management] on the web page.
- Execute [Create] in [System Settings]→[Security Settings]→[Certificate Management]→[Certificate Signing Request (CSR) Management] on the web page.
- In the setting mode of the operation panel, execute the initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine], and then restart the TOE

Also, when the TOE power is turned on, the TSF reads the encrypted RSA key stored in the internal storage and decrypts it with the storage key. The TSF holds the decrypted RSA key in the volatile memory until the TOE power is turned off and uses it for the encrypted communication.

The TSF interface related to this requirement is as follows.

- MFD power again (Recovery from power failure is treated as equivalent)

FCS_CKM.1(b)

The TSF generates a session key for communication in the negotiation of encrypted communication. The session key is composed of several keys shared between server and client each time TLS communication is performed and includes a symmetric key for encrypting / decrypting data and a MAC key for verifying the data. The TSF uses a random number generated by RBG conforming to FCS_RBG_EXT.1 to generate a 128-bit symmetric key when using the AES-128 cipher suite, or generate a 256-bit symmetric key when using the AES-256 cipher suite, then stores it in the volatile memory. It also uses a random number generated by RBG conforming to FCS_RBG_EXT.1 to generate a 160-bit MAC key when using the SHA-1 cipher suite, generate a 256-bit MAC key when using the SHA-256 cipher suite, or generate a 384-bit MAC key when using the SHA-384 cipher suite and stores it in the volatile memory.
The TSF interface related to this requirement conforms to the TSF interface of FTP_ITC.1 and FTP_TRP.1(a)/FTP_TRP.1(b).

The TSF uses a random number generated by RBG conforming to FCS_RBG_EXT.1 to generate a 256-bit key encryption key as a symmetric key for encrypting the storage key at the time of initial startup after TOE installation and reboot after TOE initialization, and stores it in the nonvolatile memory 1.
The TSF interface related to this requirement is as follows.

- Initial startup after TOE installation operation
- After performing initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine] in the settings mode of the operation panel, and reboot the TOE

The TSF uses a random number generated by RBG conforming to FCS_RBG_EXT.1 to generate a 256-bit storage key as an encryption key for encrypting data to be stored in the internal storage at the time of initial startup after TOE installation and reboot after TOE initialization, and stores it in the nonvolatile memory 2 in a state encrypted with the key encryption key stored in the nonvolatile memory 1 by using the key encryption conforming to FCS_COP.1 (f).
The TSF interface related to this requirement is as follows.

- Initial startup after TOE installation operation
- After performing initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine] in the settings mode of the operation panel, and reboot the TOE

The TSF reads the encrypted storage key stored in the nonvolatile memory 2 when the TOE power is turned on and stores the storage key decrypted with the key encryption key stored in the nonvolatile memory 1 by using the key encryption conforming to FCS_COP.1 (f) in the volatile memory for using it for the cryptographic algorithm AES Rijndael until the TOE power is turned off.
The TSF interface related to this requirement is as follows.

- Turn on the MFD power (Recovery from power failure is treated as equivalent)

FCS_CKM_EXT.4 / FCS_CKM.4

The following keys handled by TSF are discarded after becoming unnecessary.

- Asymmetric key for communication:
  The RSA key decrypted when the TOE is turned on is treated as an unnecessary key when the TOE is turned off, and is stored in volatile memory. Therefore, it is volatilezed and descarded when the TOE is turned off.
  The TSF interface related to this requirement is as follows.
  - Turn off the MFD power.
- Session key for communication:
  When TLS communication is disconnected, it is treated as an unnecessary key, and it is discarded by overwriting the area where the key is stored with a pseudo random number by a simple bit operation. Also, because it is stored on the volatile memory, it is volatilized by turning off the TOE power and discarded.
  The TSF interface related to this requirement is as follows.
  - Disconnect TLS communication started according to TSF interface of FTP_ITC.1 and FTP_TRP.1(a)/FTP_TRP.1(b).
  - Turn off the MFD power.
- Key encryption key:
  When the administrator executes initialization of private data and data in machine (Initialize Private Data / Data in Machine), the storage key is treated as an unnecessary key. At the same time the key encryption key used for encrypting / decrypting the storage key is also treated as an unnecessary key in the same way and is discarded by overwriting once with a random number generated by RBG conforming to FCS_RBG_EXT.1.
  The TSF interface related to this requirement is as follows.
  - Perform initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine] in the settings mode of the operation panel
- Storage key:
  When the administrator executes initialization of private data and data in machine (Initialize Private Data / Data in Machine), it is treated as an unnecessary key. The encrypted storage key stored in the nonvolatile memory 2 is discarded by overwriting once with a random number generated by RBG conforming to FCS_RBG_EXT.1.
  The TSF interface related to this requirement is as follows.
  - Perform initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine] in the settings mode of the operation panel

Moreover, when the TOE power is turned off, the storage key decrypted when turning on the TOE power is treated as an unnecessary key, and because it is stored on the volatile memory, it is volatilized by turning off the TOE power and discarded.
The TSF interface related to this requirement is as follows.

- Turn off the MFD power

FCS_COP.1(a)

The TSF encrypts and decrypts the communication data by operating with the CBC mode conforming to NIST SP 800-38A or the GCM mode conforming to NIST SP 800-38D for the 128-bit or 256-bit encryption key generated by FCS_CKM.1 (b) and the AES cryptographic algorithm conforming to FIPS PUB 197, for encrypting communication data in FTP_ITC.1, FTP_TRP.1 (a) and FTP_TRP.1 (b).
The TSF interface related to this requirement conforms to the TSF interface of FTP_ITC.1 and FTP_TRP.1 (a) / FTP_TRP.1 (b).

FCS_COP.1(b)

In signature generation and signature verification, the TSF uses Digital signature algorithm (DSA), RSA digital signature algorithm (rDSA) or Elliptic Curve digital signature algorithm (ECDSA) satisfying the Digital Signature Standard specified in FIPS PUB 186-4. The specific usage of each algorithm will be described below.

It uses the 2048-bit RSA key generated in accordance with FCS_CKM.1 (a) and rDSA in certificate generation by creating the TOE device certificate.

It uses rDSA with a 2048-bit key in the update verification in FPT_TUD_EXT.1.

It uses DSA, rDSA, or ECDSA in the server certificate verification in FTP_ITC.1, with a 2048- or 3072-bit DSA / rDSA key or a 256-, 384-, or 521-bit ECDSA key.

The TSF interface related to this requirement is as follows.

- Creating the TOE device certificate:
  - Initial startup after TOE installation operation
  - Execute [Create] of the device certificate from [System Settings]→[Security Settings]→[Certificate Management] →[Device Certificate Management] on the web page.
  - Perform initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine] in the settings mode of the operation panel.
- Server certificate verification:
  - Conform to the TSF interface of FTP_ITC.1
- Update verification:
  - Conform to the TSF interface of FPT_TUD_EXT.1

FCS_RBG_EXT.1

The TSF includes an RBG consisting of DRBG and ES. The DBRG is CTR_DRBG (AES-256) which satisfies NIST SP 800-90A, which requires Entropy Input containing 384 bits of entropy. This is CTR_DRBG which does not use derivation function, and other seed material (such as nonce) is not used. The ES is a self developed circuit which contains one hardware-based noise source, and generates Entropy Input containing 384 bits of entropy for entering to the DBRG.
The TSF executes repeatedly the random number generation demand and the random number read for the ES to store 384 bits or more of entropy, and generates Entropy Input containing 384 bits of entropy based on it. Then a random number used for generating encryption key is generated by providing it to the DRBG.
The TSF interface related to this requirement conforms to the TSF interface of FCS_CKM.1 (a) and FCS_CKM.1 (b).

7.3 User Data Protection

This section mainly describes the summary specification of the required FDP requirements in Section 6.2.3.

FDP_ACC.1 / FDP_ACF.1

The TSF controls access to the user data and the operation of user data.

Access control rule is implemented based on users and job owners based on Table 6.3 and Table 6.4 for operation of user data, by permitting access to the user data only for the administrator who is identified and authenticated as well as the user who is identified and authenticated and of which the user login name is coincided with the user login name linked as the owner information belonging to the user data.
The TSF interface related to D.USER.DOC access control is as shown in Table 7.3.

Table 7.3: TSF Interface related to D.USER.DOC Access Control

Function	Operation	Interface
Print	Create	• Select a document to be printed from the client PC and execute printing from the preference screen of the printer driver.
	Read	• Select the file held by Create operation from [File retrieve] on the operation panel, and execute printing. • Select the file held by Create operation from [File retrieve] on the operation panel, and execute [Check Image]. • Select the file held by Create operation from [File retrieve] on the operation panel, and execute [Change Setting to Print]. • Execute printing after the above operation.
	Modify	• Select the file held by Create operation from [File retrieve] on the operation panel, and execute editing from [Change Setting to Print].
	Delete	• Select the file held by Create operation from [File retrieve] on the operation panel, and execute [Delete]. • Select the file held by Create operation from [File retrieve] on the operation panel, and enable the setting of deleting the data after print to execute printing. • After executing Create operation, execute deleting from [System Settings]→[Security Settings]→[Data Clearance Settings]→[Clear Document Filing Data] in the settings mode of the operation panel. (Only default administrator can operate)
Scan	Create	• Place a document on the scanner unit of the MFD and execute the preview from [Easy Scan] on the operation panel. (hereinafter this operation is called Create Operation Sc1) • Place a document on the scanner unit of the MFD and execute the preview from [E-Mail] or [FTP/Desktop]. (hereinafter this operation is called Create Operation Sc2) • Place a document on the scanner unit of the MFD and execute the scan from [Easy Scan], [E-Mail] or [FTP/Desktop] on the operation panel. (hereinafter this operation is called Create Operation Sc3)
	Read	• Execute Create Operation Sc1 or Create Operation Sc2.
	Modify	• After executing Create Operation Sc2, execute editing from the preview screen.
	Delete	• After executing Create Operation Sc1 or Create Operation Sc2, execute [Scan Again] or [CA]. • After executing Create Operation Sc1 or Create Operation Sc2, press [Home Screen] button. • After executing Create Operation Sc1 or Create Operation Sc2, change mode from the mode display. • After executing Create Operation Sc3, execute [CA] or [Cancel Scan] on the operation panel. • After executing scanning, stop/delete the job created by scan execution from [Job Status]→[Scan]→[Job Queue] on the operation panel.
Copy	Create	• Place a document on the scanner unit of the MFD and execute the preview from [Easy Copy] on the operation panel. (hereinafter this operation is called Create Operation C1) • Place a document on the scanner unit of the MFD and execute the preview from [Copy] on the operation panel. (hereinafter this operation is called Create Operation C2) • Place a document on the scanner unit of the MFD and execute the copy from [Easy Copy] or [Copy] on the operation panel. (hereinafter this operation is called Create Operation C3)

Function	Operation	Interface
	Read	• Execute Create Operation C1 or Create Operation C2. • Execute the copy after the above operation. • Execute Create Operation C3.
	Modify	• After executing Create Operation C2, execute editing from the preview screen.
	Delete	• After executing Create Operation C1 or Create Operation C2, execute [Scan Again], [Scan Original Again Without change Settings] or [CA]. • After executing Create Operation C1 or Create Operation C2, press [Home Screen] button. • After executing Create Operation C1 or Create Operation C2, change mode from the mode display. • After executing Create Operation C3, execute [CA] or [Cancel Copy] on the operation panel. • After executing copying, stop/delete the job created by copy execution from [Cancel Print] or [Job Status]→[Print]→[Job Queue] on the operation panel.
Storage/retrieval	Create	• Place a document on the scanner unit of the MFD and execute Scan to Local Drive from [Easy Scan]→[Scan to USB/Local Drive], [Scan toLocal Drive], or [File retrieve]→[Scan toLoccal Drive] on the operation panel. • Specify the filing setting to be ON and execute copy or scan.
	Read	• Select a file stored by Create Operation from [File retrieve] on the operation panel and execute printing form [Print Now] or [Change Setting to Print]. • Select a file stored by Create Operation from [File retrieve] on the operation panel and execute sending form [Send].
	Modify	• Select a file stored by Create Operation from [File retrieve] on the operation panel and execute editing [Change Setting to Print]. • Select a file stored by Create Operation from [File retrieve] on the operation panel and execute editing from [Send].
	Delete	• Select a file stored by Create Operation from [File retrieve] on the operation panel and execute [Delete]. • Select a file stored by Create Operation from [Document Operations]→[Document Filing] on the web page and execute [Delete]. • Select a file stored by Create Operation from [File retrieve] on the operation panel and enable the setting of deleting the data after print to execute printing. • Execute deleting from [System Settings]→[Security Settings]→[Data Clearance Settings]→[Clear Document Filing Data] in the settings mode of the operation panel. (Only default administrator can operate)

The TSF interface related to D.USER.JOB access control is as shown in Table 7.4.

Table 7.4: TSF Interface related to D.USER.JOB Access Control

Function	Operation	Interface
Print	Create	• Select a document to be printed from the client PC and execute printing from the preference screen of the printer driver, then select the file held by print execution of the client PC from [File retrieve] on the operation panel and execute printing.
	Read	• Select [Job Status]→[Print]→[Job Queue] on the operation panel.
	Modify	N/A
	Delete	• Stop/delete the job created by Create Operation from [Cancel Print] or [Job Status]→[Print]→[Job Queue] on the operation panel.
Scan	Create	• Place a document on the scanner unit of the MFD and execute the scan from [Easy Scan], [E-Mail] or [FTP/Desktop] on the operation panel.
	Read	• Select [Job Status]→[Scan]→[Job Queue] on the operation panel.
	Modify	N/A

	Delete	• Stop/delete the job created by Create Operation from [Job Status]→[Scan]→[Job Queue] on the operation panel.
Copy	Create	• Place a document on the scanner unit of the MFD and execute the copy from [Easy Scan] or [Copy] on the operation panel.
	Read	• Select [Job Status]→[Print]→[Job Queue] on the operation panel.
	Modify	N/A
	Delete	• After executing the copy, execute [CA] or [Cancel Copy] on the operation panel during scanning original. • Stop/delete the job created by Create Operation from [Cancel Scan] or [Job Status]→[Print]→[Job Queue] on the operation panel.
Storage/retrieval	Create	(Storage Job) • Place a document on the scanner unit of the MFD and execute Scan to Local Drive from [Easy Scan]→[Scan to USB/Local Drive], [Scan toLocal Drive], or [File retrieve]→[Scan toLocal Drive] on the operation panel. (hereinafter this operation is called Create Operation S1) • Specify the filing setting to be ON and execute copy or scan. (hereinafter this operation is called Create Operation S2) (Retrieval Job) • Select a file stored by Create Operation of Storage/retrieval described in Table 7.3 from [File retrieve] on the operation panel and execute printing form [Print Now] or [Change Setting to Print]. • Select a file stored by Create Operation of Storage/retrieval described in Table 7.3 from [File retrieve] on the operation panel and execute sending from [Send].
	Read	(Storage Job) • After executing Create Operation S2, select [Job Queue] from [Print] for the copy or [Scan] for the scan in [Job Status] on the operation panel. (Retrieval Job) • Select [Job Queue] from [Print] for printing or [Scan] for transmission in [Job Status] on the operation panel.
	Modify	N/A
	Delete	(Storage Job) • After executing Create Operation S1, execute [CA] on the operation panel during scanning original. • After executing Create Operation S2, execute [Delete] of Scan job for scanning or [Delete] of Copy job for copying. (Retrieval Job) • After executing the print, stop/delete the job created by Create Operation from [Cancel Print] or [Job Status]→[Print]→[Job Queue] on the operation panel. • After executing the transmission, stop/delete the job created by Create Operation from [Job Status]→[Scan]→[Job Queue] on the operation panel.

7.4 Identification and Authentication

This section mainly describes the summary specification on the required FIA requirements in Section 6.2.4.

FIA_AFL.1

In the case of user password authentication required when operating the TOE from the operation panel or the Web page or executing printing from the client PC via the printer driver, if authentication fails three consecutive times, the authentication acceptance is stopped, That is, the user password is locked. When the elapsed time from the lock reaches 5 minutes, the lock is automatically released, that is, the number of times of authentication failure is cleared and the authentication reception is recovered from the status of stopped authentication acceptance. This requirement applies only to internal authentication.
The TSF interface related to this requirement is as follows.

- Login operation on the user authentication screen on the operation panel or the web page
- Execute printing from the PC with the printer driver for the MFD installed

FIA_ATD.1

The TSF can define and maintain user attributes like User Login Name and Authority Group.
There are two built-in authority groups, administrator authority (Admin) and user authority (User), which correspond to U.ADMIN and U.NORMAL. Built-in authority groups cannot be modified or deleted.
In addition to this, the administrator can create additional authority groups. When creating an authority group, using the built-in User authority as a model, any part can be restricted.

Only the administrator can assign each user to each authority group and create, modify, or delete authority group.

The TSF interface related to this requirement is as follows.

- Add / modify an authority group from [User Control]→[Access Control Settings]→[Authority Group] on the settings mode of the operation panel or on the web page
- Add / modify a user from [User Control] →[User Settings]→[User List] on the settings mode of the operation panel or on the web page

FIA_PMG_EXT.1

The TSF has a management function to add a user password in registering a new user and change the user password of the registered user. At this time, only the password having uppercase letters, lowercase letters, numbers, or special characters ("!", "@", "#", "$", "%", "^", "&", "*", "(" , ")") is accepted.
The TSF interface related to this requirement is as follows.

- Add / modify user from [User Control] →[User Settings]→[User List] on the settings mode of the operation panel or on the web page

The minimum password length can be specified as 15 letters or more by the default administrator.
The TSF interface related to this requirement is as follows.

- Change the minimum password length from [System Settings]→[Security Settings]→[Password Change] on the settings mode of the operation panel or on the web page

FIA_UAU.1 / FIA_UID.1

The TSF identifies and authenticates the user including the administrator when operating the TOE from the operation panel and the Web page or executing printing from the client PC via the printer driver.
The TSF supports the following two types of identification and authentication methods.

- Internal authentication method: Authentication method that uses user information registered in the TOE itself. It is always enabled.
- Network authentication method: An authentication method that uses user information registered in an external LDAP authentication server. Enabling/disabling of it can be switched by administrator.

When operating the TOE from the operation panel or the Web page, the TSF requests input of the user login name, user password and authentication destination before permitting operation of the TOE. The authentication destination can be selected in the TOE main unit only when the network authentication method is disabled, and it can be selected in the TOE main unit and the LDAP authentication server registered in the TOE when the network authentication method is enabled. It is verified at the selected authentication destination whether the entered user login name and user password are coincided with the user information registered in the selected authentication destination. However, if the entered user login name is the TOE's default administrator (admin), it is verified in the TOE main unit whether they are coincided with the default administrator information registered in the TOE main unit, regardless of the authentication destination. As a result of the verification, only when they are coincided with the registered user information, the TSF judges that it is an identified and authenticated user, and permits the user to operate the TOE in accordance with the authority group to which the user belongs. However, if the authentication destination is an LDAP authentication server and an authority group is not assigned to a user who is identified and authenticated, the user is allowed to do the operation of the TOE within the range of normal user (U.NORMAL).
When executing printing from the client PC via the printer driver, the TSF receives information of the user login name and user password entered in the preference screen of the printer driver together with the document data from the printer driver. It is verified in the TOE main unit whether the received user login

name and user password are coincided with the user information registered in the TOE main unit, when the network authentication method is disabled. It is verified in the LDAP authentication server whether they are coincided with the user information registered in the LDAP authentication server specified as the default connection destination, when the network authentication method is enabled. However, if the entered user login name is the TOE's default administrator (admin), it is verified in the TOE main unit whether they are coincided with the default administrator information registered in the TOE main unit, regardless of enabling/disabling of the network authentication method. As a result of the verification, only when they are coincided with the registered user information, the TSF judges that it is a user data input by an identified and authenticated user, and stores it in the TOE main unit. Otherwise, the TSF doesn't store the received document data in the TOE main unit and discard it.
No action is allowed until it is identified and authenticated in any identification and authentication method or interface.
The TSF interface related to this requirement is as follows.

- Login operation on the user authentication screen on the operation panel or the web page
- Execute printing from the PC with the printer driver for the MFD installed

FIA_UAU.7

In the attempt for authentication on the operation panel, the same number of asterisks (star symbols) as the characters of the entered password are displayed, but the entered characters are not displayed.
In the attempt for authentication on the web page, the input in the form of password is required for the client. This asks the client's web browser to hide the characters entered by the user in a manner like a substitute character.
The TSF interface related to this requirement is as follows.

- Login operation on the user authentication screen on the operation panel or the web page

FIA_USB.1

The TSF identifies each user by the user identification and authentication, and associates the user attributes such as the user login name and the authority group with the subject.
The TSF interface related to this requirement is as follows.

- Login operation on the user authentication screen on the operation panel or the web page

7.5 Security Management

This section mainly describes the summary specification on the required FMT requirements in Section 6.2.5.

FMT_MOF.1

The TSF permits the following management functions to be used only by an identified and authorized administrator.

- Initialize Private Data / Data in Machine

The TSF interface related to this requirement is as follows.

- Start initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine] in the settings mode of the operation panel

FMT_MSA.1

The TSF provides the function of querying the own authority group to all internal authentication users who have been identified and authenticated.
The TSF interface related to this requirement is as follows.

- Query about its own user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page

The TSF provides the function of creating, modifying and deleting the user login name and the authority group of the internal authentication user and the function of querying the user login name and the authority group of the other internal authentication user only to the administrator who has been identified and authenticated. The function of creating is provided only when registering a new internal authentication user, and the function of deleting is provided only when deleting the registered internal authentication user.

The TSF interface related to this requirement is as follows.

- Add / modify / query / delete a user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page

FMT_MSA.3

The TSF specifies the default of the belonging authority group as User, that is U.NORMAL, when newly registering an internal authentication user.
The TSF interface related to this requirement is as follows.

- Add a user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page

The TSF assigns the user login name who generate the user data as default value of the owner information of the user data when generating user data.
The TSF interface related to this requirement conforms to the TSF interface of FDP_ACC.1 / FDP_ACF.1.

FMT_MTD.1

The TSF provides a management function to change the own user password to all identified and authenticated internal authentication users.
The TSF interface related to this requirement is as follows.

- Modify its own user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page

The TSF provides the function of creating and deleting the user password of the internal authentication user and the function of modifying the user password of the internal authentication user other than himself only to the administrator. The function of creating is provided only when registering a new internal authentication user, and the function of deleting is provided only when deleting the registered internal authentication user.
The TSF interface related to this requirement is as follows.

- Add / delete the user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page

In addition to the above, the TSF provides the following functions of managing TSF data to the administrator only.

- Minimum password length (modify) *It is provided to the default administrator only
- Identification and authentication method (modify)
- Date / time (modify)
- Audit log destination (query / modify)
- Automatic logout time (query / modify)
- Address book (add / modify / delete)
- Authentication server settings (add / modify / delete)
- IP address settings (modify)
- Mail transmission server settings (query / modify)
- Scanner control firmware (query / modify)
- Print control firmware (query / modify)
- Main unit control firmware for performs Boot control of the MFD main unit (query / modify)
- Main control firmware for control of the MFD main unit (query / modify)

The TSF interface related to this requirement is as shown in the Table 7.5.

Table 7.5: TSF interface related to FMT_MTD.1

Control Function	Interface
Change minimum password length	• Change minimum password length from [System Settings]→[Security Settings]→[Password Change] in the settings mode of the operation panel or on the web page.
Change identification and authentication method	• Change authentication destination settings from [System Settings] →[Authentication Settings]→[Default Settings] in the settings mode of the operation panel or on the web page.
Set date / time	• Set date and time from [System Settings]→[Common Settings] →[Device Control]→[Clock Adjust] in the settings mode of the operation panel or on the web page.

Control Function	Interface
Set audit log destination	• Set destination from [System Settings]→[Security Settings]→[Audit Log]→[Storage/Send Settings] in the settings mode of the operation panel or on the web page.
Set automatic logout time	• Change automatic logout setting from [System Settings] →[Authentication Settings]→[Default Settings] in the settings mode of the operation panel or on the web page.
Manage address book	• Perform addition / edit / deletion from [Address Book] on the operation panel. • Perform addition / edit / deletion from [Address Book]→[Address Book] on the web page.
Set authentication server	• Add / edit / delete LDAP authentication server from [System Settings]→[Network Settings]→[LDAP Settings] in the settings mode of the operation panel or on the web page.
Set IP address	• Set IPv4 from [System Settings]→[Network Settings]→[Interface Settings] in the settings mode of the operation panel or on the web page.
Set mail transmission server	• Set from [SMTP] tab of [System Settings]→[Network Settings]→[Service Settings] in the settings mode of the operation panel or on the web page.
Update scanner control firmware	• Move to the maintenance mode on the operation panel and execute firmware update.
Update print control firmware	
Update main unit control firmware for performs Boot control of the MFD main unit	
Update main control firmware for control of the MFD main unit	

FMT_SMF.1

The TSF provides the following management functions.

- Add / delete internal authentication user
- Change user password of internal authentication user
- Change user login name of internal authentication user
- Change authority group of internal authentication user
- Set audit log destination
- Change minimum password length
- Change identification and authentication method
- Manage authority group
- Set date / time
- Set automatic logout time
- Start initialization of private data and data in machine
- Manage address book
- Set authentication server
- Set IP address
- Set mail transmission server
- Update the firmware

The TSF interface related to this requirement is as shown in the Table 7.6.

Table 7.6: TSF interface related to FMT_SMF.1

Control Function	Interface
Add / delete internal authentication user	• Add / delete user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.
Change user password of internal authentication user	• Modify user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.
Change user login name of internal authentication user	• Modify user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.
Change authority group of internal authentication user	• Modify user from [User Control] →[User Settings]→[User List] in the settings mode of the operation panel or on the web page.

Control Function	Interface
Change minimum password length	• Conform to the TSF interface of FMT_MTD.1.
Change identification and authentication method	• Conform to the TSF interface of FMT_MTD.1.
Manage authority group	• Add / modify authority group or return it to the factory default from [User Control] →[Access Control Settings]→[Authority Group] in the settings mode of the operation panel or on the web page.
Set date / time	• Conform to the TSF interface of FMT_MTD.1.
Set audit log destination	• Conform to the TSF interface of FMT_MTD.1.
Set automatic logout time	• Conform to the TSF interface of FMT_MTD.1.
Start initialization of private data and data in machine	• Conform to the TSF interface of FMT_MOF.1.
Manage address book	• Conform to the TSF interface of FMT_MTD.1.
Set authentication server	• Conform to the TSF interface of FMT_MTD.1.
Set IP address	• Conform to the TSF interface of FMT_MTD.1.
Set mail transmission server	• Conform to the TSF interface of FMT_MTD.1.
Update the firmware	• Conform to the TSF interface of FMT_MTD.1

Note that the TSF does not provide management functions related to the storage encryption. Because the storage encryption is always done.

FMT_SMR.1

The TSF has the function of authority groups regarding the roles. This function can maintain the following two roles.

- U.ADMIN role (administratrative role): the role as an administrator that has the ability to configure the security settings of this TOE. The authorization group U.ADMIN is associated with this role.
- U.NORMAL role (non-administrative role): the role as a normal user that is allowed no management functions than what affect only the user her/himself.

Only the administrator can assign each user to each authority group by FMT_MSA.1. The TSF interface related to this requirement conforms to the TSF interface of FMT_MSA.1.

7.6 Protection of the TSF

This section mainly describes the summary specification on the required FPT requirements in Section 6.2.6.

FPT_SKP_EXT.1

The TSF stores the key encryption key which is a symmetric key in plain text in the nonvolatile memory 1 but does not provide a function for reading out this key encryption key to all users including the administrator. Further, since the nonvolatile memory 1 is soldered on the board, it can not be detached.

The TSF encrypts the storage key, which is a symmetric key, with the key encryption key and stores it in the nonvolatile memory 2, then reads this encrypted storage key when the TOE power is turned on, and stores this plain text storage key decrypted with the key encryption key in the volatile memory, but does not provide the function for reading out these storage keys to all users including the administrator. In addition, the plain text storage key is volatilized and discarded when power is turned off.

The TSF stores the session key including the symmetric key and the MAC key in plain text in volatile memory, but does not provide the function for reading out this session key to all users including the administrator. Also, this session key is volatilized and discarded when power is turned off.

The TSF encrypts the private key of the TLS key pair with the storage key, saves it in the internal storage, reads the encrypted private key when the TOE is powerd on, and decrypts the plaintext private key with the storage key into volatile memory. However, it does not provide a function for reading these private keys to any users including the administrator. The plaintext private key is volatilized and destroyed when the power is turned off.

FPT_STM.1

When the TSF records audit target events indicated by FAU_GEN.1 / FAU_GEN.2 as audit logs, the TSF issues a time stamp from the system clock of the TOE.

The TSF interface related to this requirement conforms to the TSF interface of FAU_GEN.1 / FAU_GEN.2.

FPT_TST_EXT.1

The TSF performs the following self test at the start of the TOE.

- Entropy Source Health Test: In order to ensure that the ES has not failed, generate a random number of 4096 bits by repeatedly executing the random number generation demand and the random number read, and confirm that the random number generation can be completed within the specified time and that the length of the consecutive same bit value should not be more than the specified threshold value, and that bias of the appeared bit value should not exceed the tolerable range.
- DRBG Health Test: Perform Known Answer Tests on Instantiate, Generate and Reseed functions based on NIST SP 800-90A.
- HBA Encryption Circuit Test: In order to ensure that the encryption circuit has not failed, perform Known Answer Tests on AES public offering requirement (http://csrc.nist.gov/archive/aes/katmct/katmct.htm).
- TSF image verification: In order to ensure that the firmware implementing the TSF is not corrupted, self verification is performed with hash (SHA-256) for the controller firmware, and with 16-bit error detection code (checksum) for the other firmware.

If any error is detected in all or part of the above self tests, the TOE stops the start-up and suspend any operation until the power is turned off.
The TSF consists of hardware TSF and software TSF. The hardware TSF is an entropy source and HBA cryptographic circuit, and actually operates them by the entropy source health test and the HBA encryption circuit test to detect faults. The software TSF is implemented on the firmware and verifies the integrity of the TSF execution code by TSF image verification. In addition, NIST SP 800-90A which is one of the standards the TOE should follow requires self-test implementation. It is satisfied by DRBG health test. From the above, it can be said that sufficient tests are done to demonstrate that the TSF is operating correctly.
The TSF interface related to this requirement is as follows.

- Turn on the MFD power (Recovery from power failure is treated as equivalent)

FPT_TUD_EXT.1

The TSF provides the administrator with the ability to query the firmware version of the TOE and provides the default administrator with the ability to initiate the firmware update of the TOE.
Before starting the firmware update, the TSF provides the default administrator with means for verifying the authenticity of the target firmware for update. Verify the firmware authenticity by comparing the hash value decrypted by the RSA signature verification in accordance with FCS_COP.1 (b) from the digital signature provided as a part of the firmware file together with the firmware itself, and the hash value calculated by the cryptographic hashing service of SHA-256 according to file, FCS_COP.1 (c) from the state that all target firmware for update are collected together, then checking to see that those value are coincided.
The TSF interface related to this requirement is as follows.

- Query firmware version from [Status]→[Firmware Version] in the settings mode of the operation panel or on the web page
- Move to the maintenance mode on the operation panel and execute firmware update

7.7 TOE Access

This section mainly describes the summary specification on the required FTA requirements in Section 6.2.7.

FTA_SSL.3

The TSF provides a function to automatically log out after no operation for users who log in (identification and authentication) on the operation panel. The holding time is set by the administrator, and it is 10 seconds at the minimum and 240 seconds at the maximum (4 minutes).
The TSF provides a function to automatically log out after no operation for users who log in (identification and authentication) on the web page. The holding time is fixed to be 300 seconds (5 minutes).
The TSF interface related to this requirement is as follows.

- No operation after login from the user authentication screen on the operation panel or the web page

7.8 Trusted Path / Channel

This section mainly describes the summary specification on the required FTP requirements in Section 6.2.8.

FTP_ITC.1

In order to protect communication with highly reliable IT products such as the authentication server, the audit server, the FTP server and the mail server, the TSF start communication with them via trusted channel using TLS 1.2 conforming to FCS_TLS_EXT.1. This communication can be started from either the TOE or a highly reliable IT product.
The TSF initiates communication with highly reliable IT products via trusted channels for using the following functions.

- Identification and authentication by the network authentication
- Audit log data transmission
- File server transmission
- E-mail transmission

The TSF interface related to this requirement is as follows.

- Communication with the authentication server:
  - Login operation on the user authentication screen on the operation panel or the web page
- Communication with the audit server:
  - Conform to the TSF interface of FAU_GEN.1 / FAU_GEN.2
- Communication with FTP server:
  - After placing the document on the scanner unit of the MFD, perform Scan to FTP from [Easy Scan] or [FTP/Desktop] on the operation panel
  - Perform file server transmission from [Send] of [File retrieve] on the operation panel
- Communication with mail server:
  - After placing the document on the scanner unit of the MFD, perform Scan to E-mail from [Easy Scan] or [E-Mail] on the operation panel
  - Perform E-mail transmission from [Send] of [File retrieve] on the operation panel

FTP_TRP.1(a) / FTP_TRP.1(b)

The TSF establishes a trusted communication path to ensure that communication with the TOE takes place between known terminals as follows.

- The communication between the client and the TOE web page uses the HTTPS communication function to provide a trusted communication path that protects communication data from eavesdropping and the like. HTTPS communication is started by the remote administrator or remote user connecting to the TOE web page by HTTPS communication from the web browser on the client. Identification and authentication and all remote operations from the client are executed only when HTTPS communication is used.
- The communication between the printer driver of the client and the TOE uses the IPP over TLS communication function to provide a trusted communication path that protects print data to be sent from eavesdropping and the like. The communication with the TOE is started by the remote administrator or remote user connecting by IPP over TLS communication from the printer driver on the client via print operation of the application program of the client. Identification and authentication and all remote operations from the printer driver of the client are executed only when IPP over TLS communication is used.

The TSF interface related to this requirement is as follows.

- TOE remote operation for the web page
- Execute printing from the PC with the printer driver for the MFD installed

7.9 Confidential Data on Field-Replaceable Nonvolatile Storage Devices 1

This section mainly describes the summary specification on the conditionally mandatory requirements B1 in Section 6.2.9.

FPT_KYP_EXT.1

In this TOE, the keys that compose the key chain in FCS_KYC_EXT.1 are the key encryption key and the storage key.
The TSF stores the key encryption key in plain text in the nonvolatile memory 1 soldered on the board, but it is not stored in the internal storage.
The TSF stores the storage key encrypted with the key encryption key in the nonvolatile memory 2 and stores the plain text storage key decrypted with the key encryption key at the time of turning on the TOE in the volatile memory, but it is not stored in the internal storage.

FCS_KYC_EXT.1

In this TOE, BEV in the key chain is a storage key. The storage key is generated to have a 256-bit length by using a random number generated by RBG conforming to FCS_RBG_EXT.1, and encrypted / decrypted with the 256-bit key encryption key generated by using a random number generated by RBG conforming to FCS_RBG_EXT.1 by using the key encryption according to FCS_COP.1 (f). Therefore, the TSF secures security strength of 256 bits or more at each stage of the key chain.
The TSF interface related to this requirement is as follows.

- Initial start-up after TOE installation operation
- After performing initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine] in the settings mode of the operation panel, reboot the TOE
- Turn on the MFD power (Recovery from power failure is treated as equivalent)

FDP_DSK_EXT.1

When writing the document data, job information and various TSF data to the internal storage which is field replaceable nonvolatile storage, the TSF always encrypts it according to FCS_COP.1 (d) before writing it, and decrypts it when reading from the internal storage.
According to the guidance, encryption is automatically enabled by configuring this TOE in a predetermined procedure.
The internal storage has an unencrypted area. More specifically, it is a device management area such as a partition table, a boot area storing TOE firmware, and an area storing guidance. The area to be encrypted and the area not encrypted are distinguished per partition, and the user document data and the confidential TSF data are not included in the unencrypted area.
The TSF interface related to this requirement conforms to the TSF interface of FDP_ACC.1 / FDP_ACF.1 and FMT_SMF.1.

7.10 Confidential Data on Field-Replaceable Nonvolatile Storage Devices 2

This section mainly describes the summary specification on the selection-based requirements D1 in Section 6.2.10.

FCS_COP.1(d)

The TSF performs encryption and decryption of user data and TSF data according to FDP_DSK_EXT.1 as follows.

- Encryption key:
  An encryption key having a 256-bit length generated in FCS_CKM.1 (b) is used.
- Cryptographic algorithm:
  An AES algorithm specified by ISO/IEC 18033-3 and a CBC mode defined by ISO/IEC 10116 are used.

The TSF interface related to this requirement conforms to the TSF interface of FDP_DSK_EXT.1.

FCS_COP.1(f)

The TSF performs encryption and decryption according to FCS_KYC_EXT.1 in the same manner as FCS_COP.1 (d) above.
The TSF interface related to this requirement is as follows.

- Initial start-up after TOE installation operation
- After performing initialization from [System Settings]→[Security Settings]→[Initialize Private Data/Data in Machine] in the settings mode of the operation panel, reboot the TOE
- Turn on the MFD power (Recovery from power failure is treated as equivalent)

7.11 Protected Communications

This section mainly describes the summary specification on the selection-based requirements D2 in Section 6.2.11.

FCS_TLS_EXT.1

The TSF supports TLS 1.2 (RFC 5246) as TLS communication.
The cipher suite that the TSF supports in TLS communication are
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,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_
WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.
According to FCS_RBG_EXT.1 and FCS_CKM.1 (a), the TSF generates a server secret key and a public key for use in TLS communication.
The TSF performs encryption and decryption of communication data in TLS communication according to FCS_COP.1 (a).
According to FCS_COP.1 (b), the TSF performs server certificate verification in TLS communication with various servers shown in FTP_ITC.1.
According to FCS_COP.1 (c) and FCS_COP.1 (g), the TSF performs TLS communication using the Keyed-Hash Message Authentication Code (HMAC).
The TSF interface related to this requirement conforms to the TSF interface of FTP_ITC.1 and FTP_TRP.1(a)/FTP_TRP.1(b).

FCS_HTTPS_EXT.1

Since the TSF provides a trusted path according to FTP_TRP.1 (a) and FTP_TRP.1 (b) in the communication between the TOE and the remote administrator and between the TOE and the remote user, it applies HTTPS communication conforming to RFC 2818 and using the TLS protocol conforming to FCS_TLS_EXT.1.
When a remote administrator or remote user makes a connection request from the web browser on the client PC to the TOE web page, the TSF establishes the negotiation of the TLS communication between the TOE and the client PC to start HTTPS communication.
HTTPS communication is applied to identification and authentication and all remote operations on the TOE web page from the client PC.
The TSF interface related to this requirement is as follows.

- TOE remote operation for the web page

FCS_COP.1(g)

The TSF performs communication using the Keyed-Hash Message Authentication Code (HMAC), according to HMAC-SHA-1 having a 160-bit message digest length and a 160-bit key, HMAC-SHA-256 having a 256-bit message digest length and a 256-bit key, or HMAC-SHA-384 having a 384-bit message digest length and a 384-bit key which satisfies the Keyed-Hash Message Authentication Code specified in FIPS PUB 198-1 and the Secure Hash Standard specified in FIPS PUB180-3.
Cryptographic hashing service of SHA-1, SHA-256 or SHA-384 according to FCS_COP.1 (c) is used for hashing to calculate a hash value.
The TSF interface related to this requirement conforms to the TSF interface of FCS_TLS_EXT.1 and FTP_TRP.1(a)/FTP_TRP.1(b).

7.12 Trusted Update

This section mainly describes the summary specification on the selection-based requirements D3 in Section 6.2.12.

FCS_COP.1(c)

The TSF uses a cryptographic hashing service according to SHA-1, SHA-256, SHA-384, or SHA-512 which conforms to ISO/IEC 10118-3:2004 for calculating hash values below.

- Signature verification by FCS_COP.1(b) in FPT_TUD_EXT.1: SHA-256
- Signature generation by FCS_COP.1(b) in FCS_TLS_EXT.1: SHA-256
- Signature verification by FCS_COP.1(b) in FCS_TLS_EXT.1: SHA-1 / SHA-256 / SHA-384 / SHA-512
- HMAC by FCS_COP.1(g) in FCS_TLS_EXT.1: SHA-1 / SHA-256 / SHA-384

The TSF interface related to this requirement conforms to the TSF interface of FPT_TUD_EXT.1, FCS_TLS_EXT.1 and FCS_CKM.1(a) RSA key generation.

8 Appendix

This chapter describes the reference documents and the definitions of terms.

8.1 Terminology

Among terminology used in this ST, the terms defined in CC and PP conforming in Chapter 2 follow the definitions of them. The terms other than that are defined in Table 8.1.

Table 8.1: Definition of terms used in this ST

Term	Definition
Board	A printed circuit board on which components are mounted by soldering.
Controller firmware	A firmware that controls the controller unit in the MFD.
Controller unit	A device that controls the whole MFD. It contains the CPU, volatile memory, HBA, ES, nonvolatile memory and others for executing firmware of the TOE.
Document filing	A function that stores image data that the MFD handles into the internal storage for enabling users to retrieve later.
Engine unit	A device that forms print images on receiver papers, with mechanism of paper feeding / ejection.
Firmware	A software that is embedded to the machines to control the machine's hardware.
Image data	A digital data, especially in this document, of two-dimensional image that each function of the MFD manages.
Internal authentication user	A user registered in the TOE main unit which is referenced at the internal authentication.
IP address	A call sign, used for IP, to identify devices for communication.
Lock	A status in which password acceptance is stopped because wrong passwords are entered in a row.
Memory	A memory device; in particular a semiconductor memory device.
Nonvolatile memory	A memory device that retains its contents even when the power is turned off.
Operation panel	A user interface unit in front of the MFD. This contains the function key and liquid crystal display with touch operation system.
Retrieving	For the image data stored by the document filing function, performing operations such as print, send, preview and delete.
Rijndael	A cryptographic algorithm adopted by the AES. The developers are Joan Daemen and Vincent Rijmen from Belgium.
Scan to Local Drive	One of the document filing functions. It scans the original to obtain image data, and store the image data into the internal storage, but neither prints nor sends it.
Scanner unit	A device that scans the original and gets the image data. This is used for copy, scan transmission or scan toLocal Drive.
Spool	Storing the image data of the job into the internal storage temporarily to increase the input and output efficiency.
Unit	A unit that is equipped with removable standard items and optional items on a printed circuit board and is in an operable state. Also, a unit that is made operable including the mechanical section.
Volatile memory	A memory device in which the contents vanish when the power is turned off.
TOE web page / Web page	A web page provided by the web server built in the MFD as the remote operation I/F of the MFD which is the TOE.

8.2 Abbreviations

Abbreviations used in this ST are indicated in Table 8.2.

Table 8.2: Definition of abbreviations used in this ST

Abbreviation	Definition
AES	Advanced Encryption Standard
BEV	Border Encryption Value
CC	Common Criteria
CM	Configuration Management
CPU	Central Processing Unit

Abbreviation	Definition
DRBG	Deterministic Random Bit Generator
ES	Entropy Source
FIPS PUB 197	Federal Information Processing Standards Publication 197
HBA	Host Bus Adapter
HCD	Hardcopy Device
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL/TLS
I/F	Interface
IP	Internet Protocol
IPP	Internet Printing Protocol
IPP-SSL	IPP over SSL/TLS
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MFD	Multifunction Device
MFP	Multifunction Printer, Multifunction Peripheral
NIC	Network Interface Card, Network Interface Controller
OS	Operating System
PC	Personal Computer
PP	Protection Profile
RBG	Random Bit Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality