Fuji Xerox ApeosPort 3560/3060/2560/ 3560 G/3060 G/2560 G models with Copy, Print, Fax, Scan and Overwrite Storage Security Target

Version 1.07

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

January 2021

- Table of Contents -

1. ST INTRODUCTION 1
1.1. ST Reference 1
1.2. TOE Reference 1
1.3. TOE Overview 3
1.3.1. TOE Type 3
1.3.2. Usage and Major Security Features of TOE 3
1.3.3. Required Non-TOE Hardware and Software 4
1.4. TOE Description 6
1.4.1. Users Assumptions 6
1.4.2. Logical Boundary of the TOE 7
1.4.3. Physical Boundary of the TOE 9
2. CONFORMANCE CLAIM 12
2.1. CC Conformance Claim 12
2.2. PP claim, Package Claim 12
2.2.1. PP Claim 12
2.2.2. Package Claim 12
2.2.3. Conformance Rationale 12
3. SECURITY PROBLEM DEFINITION 13
3.1. Threats 13
3.1.1. Assets Protected by TOE 13
3.1.2. Threats 13
3.2. Organizational Security Policies 14
3.3. Assumptions 15
4. Security Objectives 16
5. EXTENDED COMPONENTS DEFINITION 17
5.1. Extended Functional Requirements Definition 17
5.1.1. Class FAU: Security Audit 17
5.1.2. Class FCS: Cryptographic Support 18
5.1.3. Class FDP: User Data Protection 23
5.1.4. Class FIA: Identification and Authentication 25
5.1.5. Class FPT: Protection of the TSF 26
6. SECURITY REQUIREMENTS 30
6.1. Notation 30
6.2. Security Functional Requirements 30
6.2.1. Class FAU: Security Audit 30
6.2.2. Class FCS: Cryptographic Support 33

6.2.3. Class FDP: User Data Protection 41
6.2.4. Class FIA: Identification and Authentication 45
6.2.5. Class FMT: Security Management 47
6.2.6. Class FPT: Protection of the TSF 51
6.2.7. Class FTA: TOE Access 52
6.2.8. Class FTP: Trusted Paths/Channels 53
6.3. Security Assurance Requirements 55
6.4. Security Requirement Rationale 56
6.4.1. Dependencies of Security Functional Requirements 56
6.4.2. Security Assurance Requirements Rationale 60
7. TOE Summary Specification 61
7.1. Security Functions 61
7.1.1. Identification and Authentication 63
7.1.2. Security Audit 65
7.1.3. Access Control 69
7.1.4. Security management 71
7.1.5. Trusted Operation 73
7.1.6. Data Encryption 74
7.1.7. Trusted Communications 80
7.1.8. PSTN Fax-Network Separation 83
7.1.9. Overwrite Storage 83
8. ACRONYMS AND TERMINOLOGY 84
8.1. Acronyms 84
8.2. Terminology 84
9. REFERENCES 89

- List of Figures and Tables -

Figure 1 Operational Environment Assumed by TOE 3
Figure 2 TOE Logical Boundary 7

Table 1 User Roles 6
Table 2 Physical Components Constituting the TOE (MFD Main Unit) 10
Table 3 Physical Components Constituting the TOE (Japanese version guidance) 11
Table 4 Physical Components Constituting the TOE (English version guidance) 11
Table 5 Assets for User Data 13
Table 6 Assets for TSF Data 13
Table 7 Threats 13
Table 8 Organizational Security Policies 14
Table 9 Assumptions 15
Table 10 Security Objectives for the TOE Environment 16
Table 11 Auditable Events 31
Table 12 D.USER.DOC Access Control SFP 42
Table 13 D.USER.JOB Access Control SFP 43
Table 14 List of Security Functions 48
Table 15 Security Attributes and Authorized Roles 48
Table 16 Management of TSF Data 49
Table 17 Security Management Functions 50
Table 18 Security Assurance Requirements 55
Table 19 Dependencies of Functional Security Requirements 56
Table 20 Security Functional Requirements and the Corresponding TOE Security Functions 61
Table 21 Details of Security Audit Log 66
Table 22 Security management functions and their operationable UIs 71
Table 23 Methods to destroy keys and key material stored in plaintext 75

1. ST INTRODUCTION

This chapter describes Security Target (ST) Reference, TOE Reference, TOE Overview, and TOE Description.

1.1. ST Reference

This section provides information needed to identify this ST.

ST Title:	Fuji Xerox ApeosPort 3560/3060/2560/3560 G/3060 G/2560 G models with Copy, Print, Fax, Scan and Overwrite Storage Security Target
ST Version:	V 1.07
Publication Date:	January 12, 2021
Author:	Fuji Xerox Co., Ltd.

1.2. TOE Reference

This section provides information needed to identify the TOE.

TOE Identification:	Fuji Xerox ApeosPort 3560/3060/2560/3560 G/3060 G/2560 G models with Copy, Print, Fax, Scan and Overwrite Storage
Version:	Controller ROM Ver. 1.5.3, FAX ROM Ver. 2.2.1

The TOE is one of the following products.

Japanese market

Product	Version
ApeosPort 3060 models with Copy, Print, Fax, Scan and Overwrite Storage	Controller ROM Ver. 1.5.3, Fax ROM Ver.2.2.1
ApeosPort 2560 models with Copy, Print, Fax, Scan and Overwrite Storage	

Other markets

Product	Version
ApeosPort 3560 models with Copy, Print, Fax, Scan and Overwrite Storage	Controller ROM Ver. 1.5.3, Fax ROM Ver.2.2.1
ApeosPort 3060 models with Copy, Print, Fax, Scan and Overwrite Storage	
ApeosPort 2560 models with Copy, Print, Fax, Scan and Overwrite Storage	

ApeosPort 3560 G models with Copy, Print, Fax, Scan and Overwrite Storage	
ApeosPort 3060 G models with Copy, Print, Fax, Scan and Overwrite Storage	
ApeosPort 2560 G models with Copy, Print, Fax, Scan and Overwrite Storage	

1.3. TOE Overview

1.3.1. TOE Type

The TOE is an MFD that is connected to a wired Local Area Network (LAN) and supports the copy, scan, print, fax, and document storage and retrieval functions.

1.3.2. Usage and Major Security Features of TOE

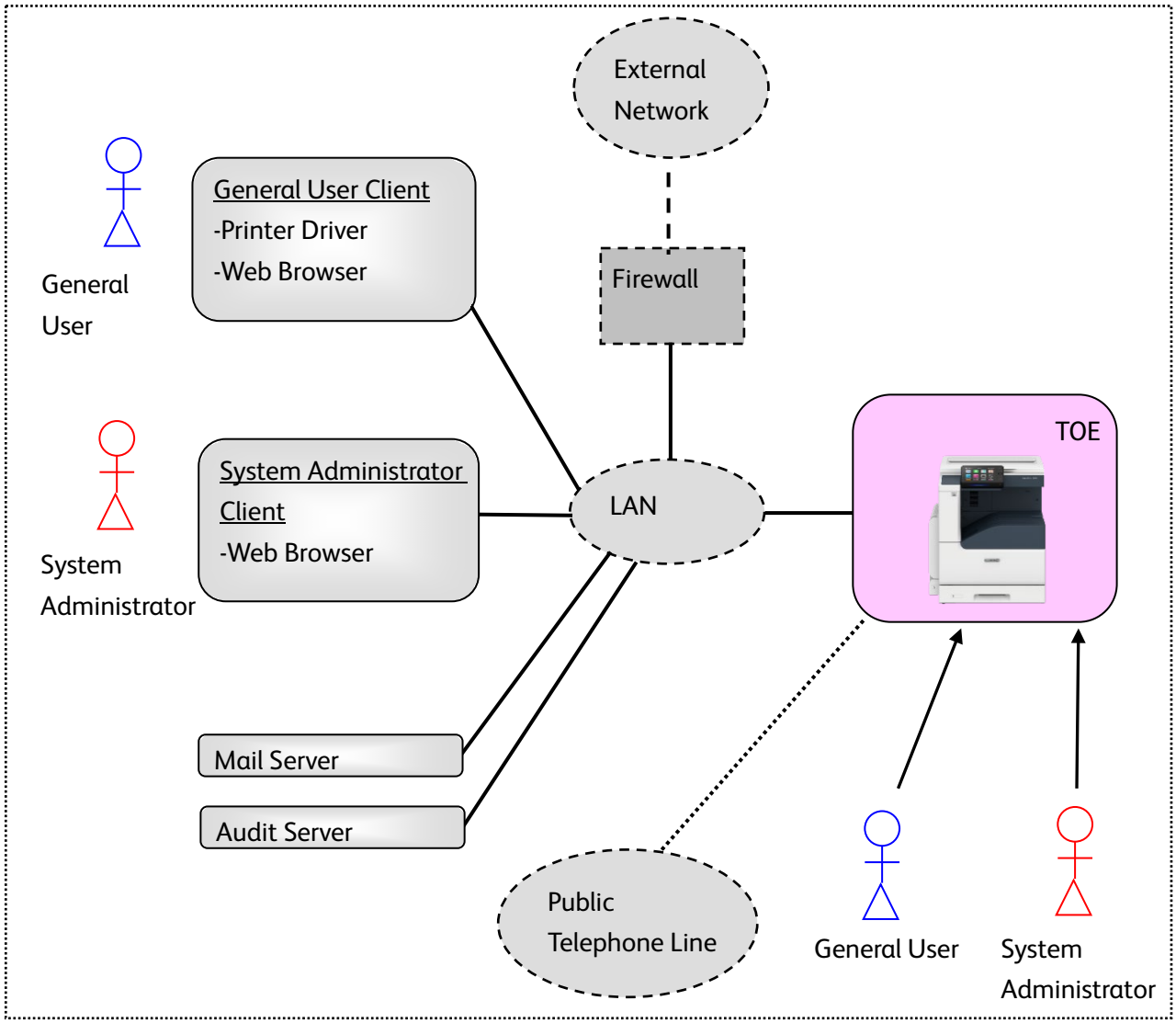


Figure 1 Operational Environment Assumed by TOE

The MFD is used in an environment that is connected to a wired Local Area Network (LAN) isolated from the external network by the firewall.
The MFD can connect to the public telephone line to send and receive fax data.

Users use each basic function of the MFD from the control panel of the MFD or web browser or printer driver of the general user and system administrator clients.
The MFD has the functions to copy, scan, print, fax (send and receive), store and retrieve the documents handled by users.
To prevent alteration and leakage of these documents, the MFD has the functions to identify and authenticate users, control access to documents and functions based on user roles, encrypt the setting data and document data stored in MFD storage, protect the communication data on the LAN, manage security settings (available only to system administrators), store the usage history of the security functions of the MFD in the MFD internally and monitor the usage history from an external audit server at the same time (security audit function), verify the integrity of the TSF executable code and TSF data, verify the authenticity of the TSF executable code when the code is updated, and separate the fax line and the LAN, and overwrite residual image data stored in the storage.
To use overwrite residual image data function, it is necessary to purchase the data overwrite kit and enable the overwrite storage function.

The products that are included in the TOE support local authentication and remote authentication, when the remote authentication option is installed. However, only local authentication is used in the settings of the TOE.

Note:

- There are two types of Mailboxes: The Personal Mailbox, which SAs and general users can create, and the Shared Mailbox, which the Key Operator can create. The guidance of the TOE prohibits the use of the Shared Mailbox. In this ST, "Mailbox" means "Personal Mailbox."
- The interfaces for users to connect personal storage devices (portable flash memory devices, etc.) to the MFD are disabled.

1.3.3. Required Non-TOE Hardware and Software

In the operational environment shown in Figure 1, the TOE is an MFD, and there are the following non-TOE hardware and software.

(1) General user client

The hardware is a general-purpose computer.
When the computer is used as a printer client, the user needs to install a printer driver on the computer so that a request to print document data can be sent to the MFD.
In order to use the web server function of the MFD, the user needs to use a web browser installed on the computer.

(2) System administrator client

The hardware is a general-purpose computer.

A web browser is necessary for a system administrator to refer to and change the TOE settings and update the TOE firmware.

(3) Mail server

A mail server is necessary for the MFD to send scanned documents via email. The hardware/OS of the server is a general-purpose computer/server, and an email service that supports the SMTP protocol protected by TLS needs to be installed.

(4) Audit server

An audit server is necessary to collect audit events occurred on the MFD. The hardware/OS is a general-purpose computer/server, and the MFD sends security audit logs to the audit server using HTTPS on the request of the audit server.

In the TOE evaluation, the following shall be used as the hardware and software listed above.
The OS and web browser for (1) general user client and (2) system administrator client shall be Windows 10 and Microsoft Edge respectively.
(3) mail server shall be Postfix version 2.10.1.
The OS of (4) audit server shall be Windows 10, and the execution environment to retrieve logs shall be PowerShell version 5.1. The system administrator needs to create a PowerShell script for log retrieval in accordance with the guidance and install it on the server.
The printer driver used in (1) general user client shall be either of the following printer drivers, which Fuji Xerox offers for the target MFD models.
For the Japanese market: ART EX Driver (Microsoft® WHQL Certified Driver)
For other markets: 64-bit Windows Print Driver (PCL)

1.4. TOE Description

This section describes user roles and the logical and physical boundaries of the TOE.

1.4.1. Users Assumptions

Table 1 specifies the TOE user roles assumed in this ST.

Table 1 User Roles

Name	User data type	Definition
U.NORMAL	General user	An identified and authorized User who is not granted the administrative role.
U.ADMIN	System administrator	An identified and authorized User who is granted the administrative role. (In the TOE, the Key Operator and SAs are U.ADMIN. They are collectively referred to as U.ADMIN in this ST.)

1.4.2. Logical Boundary of the TOE

Figure 2 shows the logical architecture of the TOE.
Among the functions within the logical boundary, the ones without underlines are basic functions and the ones with underlines are security functions.

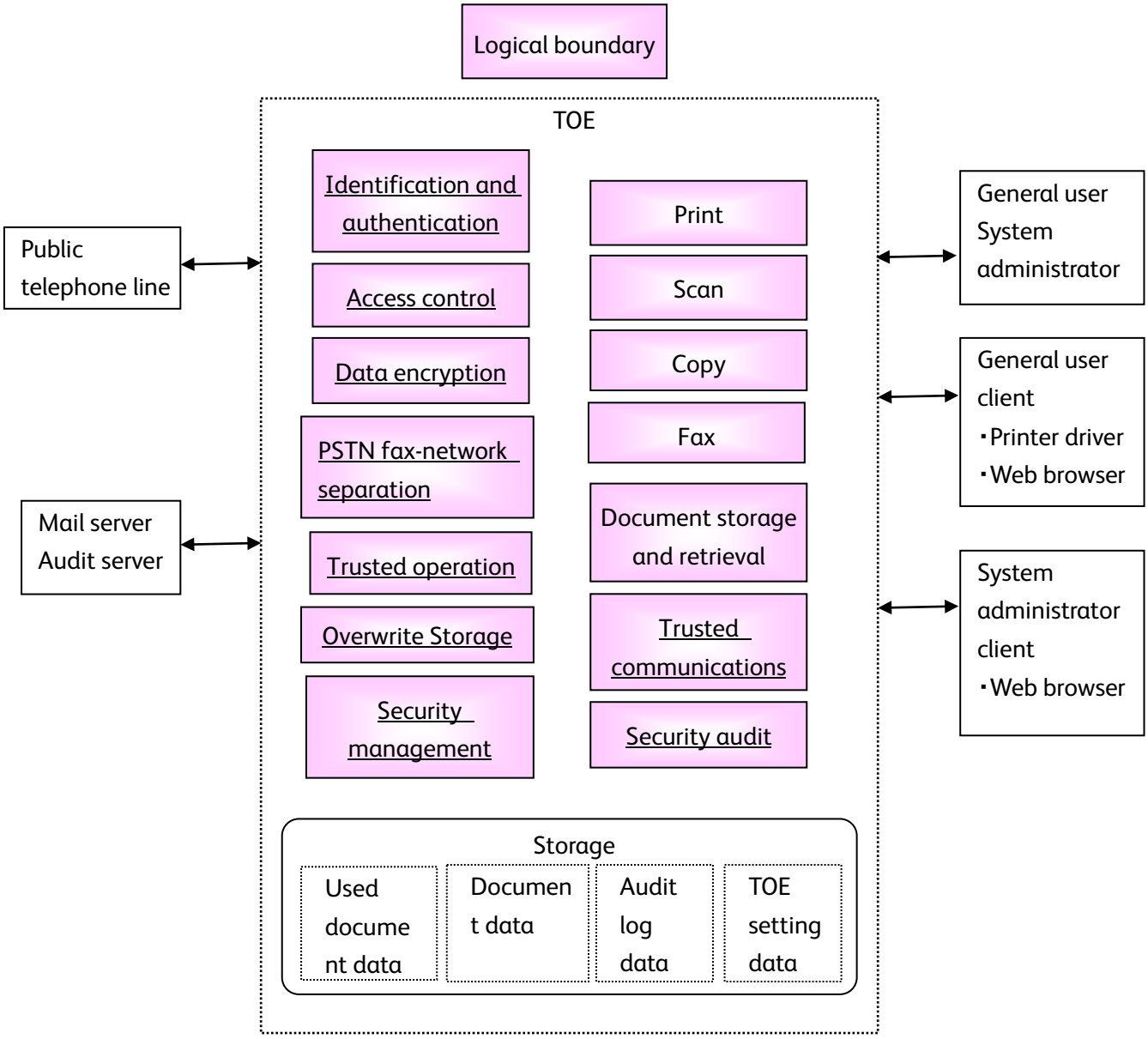


Figure 2 TOE Logical Boundary

1.4.2.1. Basic Functions

(1) Print: The MFD receives a digital document sent from the printer driver of the general user client. The received document is converted into a hard copy in accordance with the request from the control panel.

(2) Scan: The MFD scans the document on the scanner in accordance with the request from the control panel and converts the document into a digital document. The TOE has the function to send digital documents converted from paper documents by the scan function

to the mail server and the function to store these documents in Mailboxes using the document storage and retrieval function.

(3) Copy: The MFD copies the document on the scanner in accordance with the request from the control panel.

(4) PSTN fax send: The MFD scans the document on the scanner in accordance with the request from the control panel and sends the document data to the PSTN fax destination through PSTN using the standard PSTN fax protocol.

(5) PSTN fax receive: The MFD receives fax document data sent from the machine on the other end of line through PSTN and stores the data in a specific Mailbox using the document storage and retrieval function.

(6) Document storage and retrieval: The MFD stores digital documents in Mailboxes and enables the following functions for stored documents in response to requests sent from the control panel or general user clients. In the TOE, digital documents that can be stored in a Mailbox are scanned documents with the scan function, or fax documents received with the PSTN fax receive.
Print: Print a digital document stored in Mailbox in accordance with the request from the control panel.
Retrieve: Send documents to general user clients in response to requests sent from general user clients.
Delete: Delete stored digital documents in accordance with the request from the control panel or general user clients.

1.4.2.2. Security Functions

The TOE provides the following security functions to support the basic functions described in 1.4.2.1.

(1) Identification and Authentication
Identifying/authenticating users and granting roles to the users ensure that functions of the MFD are accessible only to users who have been granted roles by a system administrator. The user identification and authentication function are also used as the basis for access control and administrative roles and helps associate specific users with security-relevant events and records of MFD use. The MFD carries out the identification and authentication of users.
When a user attempts to be authenticated and fails consecutively multiple times, another request to authenticate the user is no longer accepted.
When the remote authentication option is additionally installed, the products that are included in the TOE support local authentication and remote authentication. However, only local authentication is selected in the TOE settings.

(2) Access Control
Access control ensures that documents, information related to document processing, and security-relevant data are accessible only to users who have appropriate access permissions.

(3) Data Encryption

Data encryption ensures that the data and communications data stored in the TOE cannot be accessed by an attacker through an unauthorized interface.

- Depending on the policy, data encryption is also used to protect documents and confidential system information on field-replaceable nonvolatile storage devices and to protect such data when these devices are removed from the MFD.
- The effectiveness of data encryption is assured through the use of internationally accepted cryptographic algorithms.

(4) Trusted Communications

Trusted communications protect communication data on an internal network, such as document data, job information, security audit log data, and TOE setting data.
The TOE supports general encrypted communication protocols (TLS/HTTPS and TLS).

(5) Security Management

The security management function ensures that only users who have been identified and authenticated as system administrators can refer to or change the settings of security functions of the TOE from the control panel or system administrator client.

(6) Security Audit

Information about when and who carried out which actions and important events, such as device failure, configuration change, and user operation, are transferred to the audit server and stored as security audit log data. The security audit log data is encrypted by the HTTPS protocol when being transferred.
The history of audit log data is stored in the TOE internally, only authorized users as a system administrator can also download it from a web browser of a system administrator client.

(7) Trusted Operation

Firmware updates for the MFD are verified before being applied to ensure the authenticity of the software. The MFD performs self-tests to ensure that its operation is not disrupted by some detectable malfunctions.

(8) PSTN Fax-Network Separation

With regard to PSTN fax-network separation, the MFD ensures that the PSTN fax modem is not used to create a data bridge between the PSTN and the LAN.

(9) Overwrite Storage

Used document data stored in the internal storage is overwritten after any of functions, such as copy, print, and scan, is completed.

1.4.3. Physical Boundary of the TOE

The physical boundary of the TOE is the whole MFD. The TOE does not include options and add-ons that are not relevant to security, such as finishers. Physical components that constitute the TOE are listed in Tables 2 to 4.
MFD unit is identified by the model name located on the front side of the enclosure cover of the unit and function buttons displayed in the control panel after start-up.

Table 2 Physical Components Constituting the TOE (MFD Main Unit)

Market	Unit	Version	Format	Delivery method
Japan/ Other	ApeosPort 2560 models with Copy, Print, Fax, Scan and Overwrite Storage	Controller ROM Ver. 1.5.3, FAX ROM Ver. 2.2.1	Hardware on which firmware in binary format is installed	On-site
Japan/ Other	ApeosPort 3060 models with Copy, Print, Fax, Scan and Overwrite Storage	Controller ROM Ver. 1.5.3, FAX ROM Ver. 2.2.1	Hardware on which firmware in binary format is installed	On-site
Other	ApeosPort 3560 models with Copy, Print, Fax, Scan and without Overwrite Storage	Controller ROM Ver. 1.5.3, FAX ROM Ver. 2.2.1	Hardware on which firmware in binary format is installed	On-site
Other	ApeosPort 2560 G models with Copy, Print, Fax, Scan and without Overwrite Storage	Controller ROM Ver. 1.5.3, FAX ROM Ver. 2.2.1	Hardware on which firmware in binary format is installed	On-site
Other	ApeosPort 3060 G models with Copy, Print, Fax, Scan and without Overwrite Storage	Controller ROM Ver. 1.5.3, FAX ROM Ver. 2.2.1	Hardware on which firmware in binary format is installed	On-site
Other	ApeosPort 3560 G models with Copy, Print, Fax, Scan and without Overwrite Storage	Controller ROM Ver. 1.5.3, FAX ROM Ver. 2.2.1	Hardware on which firmware in binary format is installed	On-site

As shown in Table 3 and Table 4, the guidance of this TOE is available in Japanese and English. The Japansese version for the Japanese market and the English version for other markets are distributed to users.

Table 3 Physical Components Constituting the TOE (Japanese version guidance)

Form number	Format	Delivery method	Guidance name	Hash value
ME8976J1-1	PDF file	Web	ApeosPort 3060 ApeosPort 2560 ApeosPort 1860 User Guide	7618bfd611909fbd15e369148b71a279a20ed94a7de37b2bfc6f85fa04d5226c
DE6678J1-2	Paper	On-site	ApeosPort 3060 / ApeosPort 2560 / ApeosPort 1860 Setup Guide	-
ME8816J1-1_20210112	PDF file	Web	ApeosPort 3060 ApeosPort 2560 Security Function Supplementary Guide	13274786137adef81d8356be4791d9c40750b47cf7282ba0b8dabdea40fc5774

Table 4 Physical Components Constituting the TOE (English version guidance)

Form number	Format	Delivery method	Guidance name	Hash value
ME8814E2-1	PDF file	Web	ApeosPort 3560 ApeosPort 3060 ApeosPort 2560 User Guide	cf2ce576da0bc1c1e5a2ae6e5085e3e89dc234a3dd0b628b142baf25c94b893b
DE6678W6-1	Paper	On-site	ApeosPort 3560 / 3060 / 2560 Setup Guide	-
ME8817E2-1_20210112	PDF file	Web	ApeosPort 3560 ApeosPort 3060 ApeosPort 2560 Security Function Supplementary Guide	cfad495614c3e4c2534308a95ec438a3ffd43f8e60959ae1c5c54b670086ec7a

2. CONFORMANCE CLAIM

2.1. CC Conformance Claim

This ST and TOE claim conformance to the following versions of CC:

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model (April 2017 Version 3.1 Revision 5)
Part 2: Security functional components (April 2017 Version 3.1 Revision 5)
Part 3: Security assurance components (April 2017 Version 3.1 Revision 5)

CC Part2 extended
CC Part3 conformant

2.2. PP claim, Package Claim

2.2.1. PP Claim

This ST claims exact conformance to the following HCD-PP.

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

2.2.2. Package Claim

This Security Target and TOE do not claim package conformance.

2.2.3. Conformance Rationale

This ST and TOE satisfy the conditions required by the PP.
The TOE type conforms to the PP because this ST and TOE satisfy the following conditions required by the PP and claim exact conformance to the PP.

- Required Uses
  Printing, scanning, copying, network communications, administration
- Conditionally Mandatory Uses
  PSTN faxing, storage and retrieval, field-replaceable nonvolatile storage.
- Optional Uses
  Internal audit log storage, Image Overwrite

3. SECURITY PROBLEM DEFINITION

This chapter describes the threats, organizational security policies, and the assumptions for the use of the TOE.

3.1. Threats

3.1.1. Assets Protected by TOE

The TOE protects the following assets.

Table 5 Assets for User Data

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

Table 6 Assets for TSF Data

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

3.1.2. Threats

Table 7 identifies the threats addressed by the TOE.

Table 7 Threats

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.

T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.2. Organizational Security Policies

Table 8 describes the organizational security policies the TOE must comply with.

Table 8 Organizational Security Policies

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

3.3. Assumptions

Table 9 describes the assumptions for the performance, operation, and use of the TOE.

Table 9 Assumptions

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

4. Security Objectives

This chapter describes the security objectives for the environment. Table 10 defines the security objectives for the TOE environment.

Table 10 Security Objectives for the TOE 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

Extended components in this section are defined in HCD-PP.

5.1. Extended Functional Requirements Definition

5.1.1. Class FAU: Security Audit

FAU_STG_EXT Extended: External Audit Trail Storage

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

Component leveling:

FAU_STG_EXT.1 Extended: External Audit Trail Storage interfaces	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 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.

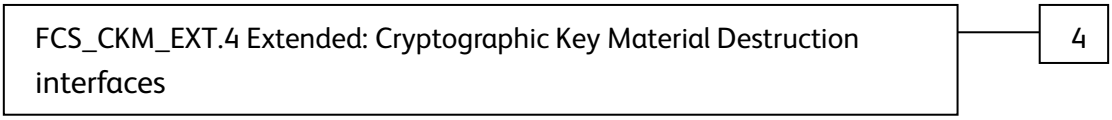
This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

5.1.2. Class FCS: Cryptographic Support

FCS_CKM_EXT Extended: Cryptographic Key Management

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

Component leveling:



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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FCS_CKM_EXT.4 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.

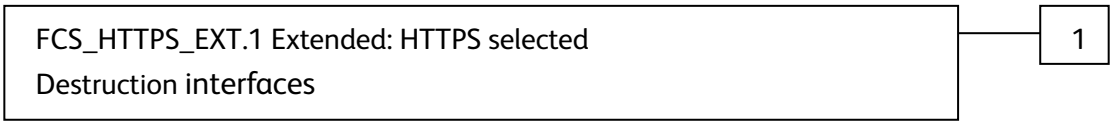
Rationale:
Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.

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.

FCS_HTTPS_EXT Extended: HTTPS selected

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

Component leveling:



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

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

- There are no management actions foreseen.

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

- Failure of HTTPS session establishment

FCS_HTTPS_EXT.1	**HTTPS selected**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

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

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

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 Extended: Key Chaining	1

FCS_KYC_EXT.1 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 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-bit and 256-bit].

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.

FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

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

Component leveling:

FCS_RBG_EXT.1 Extended: Random Bit Generation	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FCS_RBG_EXT.1 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.

FCS_TLS_EXT Extended: TLS selected

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

Component leveling:

FCS_TLS_EXT.1 Extended: TLS selected	1

FCS_TLS_EXT.1 TLS selected, requires the TLS protocol implemented as specified.

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

- There are no management actions foreseen.

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

- Failure of TLS session establishment

FCS_TLS_EXT.1 Extended: TLS selected

Hierarchical to:	No other components.
Dependencies:	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 cipher suites:

Mandatory cipher suites:
TLS_RSA_WITH_AES_128_CBC_SHA

Optional cipher suites:
[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.

5.1.3. Class FDP: User Data Protection

FDP_DSK_EXT Extended: Protection of Data on Disk

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

Component leveling:

FDP_DSK_EXT.1 Extended: Protection of Data on Disk	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 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.

FDP_FXS_EXT Extended: Fax Separation

Family Behavior:
This family addresses the requirements for separation between PSTN fax line and the LAN to which TOE is connected.

Component leveling:

FDP_FXS_EXT.1 Extended: Fax Separation	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FDP_FXS_EXT.1 Fax separation

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

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

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

5.1.4. Class FIA: Identification and Authentication

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 Extended: Password Management	1

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

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FIA_PMG _EXT.1 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.

5.1.5. Class FPT: Protection of the TSF

FPT_KYP_EXT Extended: Protection of Key and Key Material

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

Component leveling:

FPT_KYP_EXT.1 Extended: Protection of key and key material	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 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.

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 Extended: Protection of TSF Data	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_SKP_EXT.1 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.

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 Extended: TSF testing	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FPT_TST_EXT.1 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. 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.

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 Extended: Trusted Update	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update

Hierarchical to:	No other components.
Dependencies:	[FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), or FCS_COP.1(c) Cryptographic operation (Hash Algorithm)].

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

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

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

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

6. SECURITY REQUIREMENTS

This chapter describes the security functional requirements, security assurance requirements, and security requirement rational.
The definitions of terms used in this chapter are as follows.

6.1. Notation

Bold typeface indicates the portion of an SFR that has been completed or refined in HCD-PP, relative to the original SFR definition in Common Criteria Part 2 or to its Extended Component Definition.
Bold italic typeface indicates the portion of an SFR that has been partially completed or refined in HCD-PP. It also must be selected and/or completed in this ST.
Underlined bold italic typeface in parentheses that follows **underlined bold** typeface indicates the portion of an SFR that has been partially completed in HCD-PP and refined in this ST.
Italic typeface indicates the text within an SFR that must be selected and/or completed in this ST.
Gray italic typeface indicates the text within an SFR that has not been selected in this ST.
Underlined italic typeface indicates the text within an SFR that has been assigned in this ST.

The definition of SFR components followed by (a), (b)… is as described in the PP. SFR components followed by (a1), (a2)… represent required iterations of iterations.

6.2. Security Functional Requirements

Security functional requirements provided by the TOE are described below.

6.2.1. Class FAU: Security Audit

FAU_GEN.1	**Audit data generation** (for O.AUDIT)
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **not specified** level of audit; and c) **All auditable events specified in Table 11**, [assignment: *no other auditable events*].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 11**, [assignment: *no other relevant information*].

Table 11 Auditable Events

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

FAU_GEN.2 **User identity association**
(for O.AUDIT)

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

FAU_SAR.1 **Audit review**
(for O.AUDIT)

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

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

FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
FAU_SAR.2	**Restricted audit review** (for O.AUDIT)
Hierarchical to: Dependencies:	No other components. FAU_SAR.1 Audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
FAU_STG.1	**Protected audit trail storage** (for O.AUDIT)
Hierarchical to: Dependencies:	No other components. FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.
FAU_STG.4	**Prevention of audit data loss** (for O.AUDIT)
Hierarchical to: Dependencies:	FAU_STG.3 Action in case of possible audit data loss FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	**Refinement**: The TSF shall [selection, choose one of: "~~***ignore audited events***~~", "*prevent audited events, except those taken by the authorised user with special rights*", "***overwrite the oldest stored audit records***"] and [assignment: *no other actions to be taken*] if the audit trail is full.
FAU_STG_EXT.1	**Extended: External Audit Trail Storage** (for O.AUDIT)
Hierarchical to: Dependencies:	No other components. 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. Class FCS: Cryptographic Support

FCS_CKM.1(a)	**Cryptographic Key Generation (for asymmetric keys)** (for O.COMMS_PROTECTION)
Hierarchical to:	No other components.
Dependencies:	[FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), or FCS_COP.1(i) Cryptographic operation (Key Transport)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_CKM.1.1(a)	Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with** [**selection:** ***• NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*** ***• NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*** ***• NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes*** **] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.**
FCS_CKM.1(b)	**Cryptographic key generation (Symmetric Keys)** (for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)
Hierarchical to:	No other components.
Dependencies:	[FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption), or

	FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption), or FCS_COP.1(e) Cryptographic Operation (Key Wrapping), or FCS_COP.1(f) Cryptographic operation (Key Encryption), or FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication), or FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FCS_CKM.1.1(b)	Refinement: The TSF shall generate symmetric cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [selection: *128-bit*, *256-bit*] that meet the following: No Standard.**
FCS_CKM.4	**Cryptographic key destruction** (for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
Hierarchical to: Dependencies:	No other components. [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM.4.1	Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**selection:** ***For volatile memory, the destruction shall be executed by [selection: powering off a device**, [assignment: other mechanism that ensures keys are destroyed]***]. ***For nonvolatile storage, the destruction shall be executed by a [selection: single**, three or more times**] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1)**, a static pattern**], followed by a [selection:** read-verify**, none]. If read-verification of the overwritten data fails, the process shall be repeated again;**

	] that meets the following: [**selection**: *NIST SP800-88, **no standard***].
FCS_CKM_EXT.4	**Cryptographic Key Material Destruction** (for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
Hierarchical to: Dependencies:	No other components. [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_COP.1(a)	**Cryptographic Operation (Symmetric encryption/decryption)** (for O.COMMS_PROTECTION)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys) FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(a)	Refinement: The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in** [**assignment:** *CBC, GCM*] and cryptographic key sizes **128-bits and 256-bits** that meets the following: **FIPS PUB 197, "Advanced Encryption Standard (AES)"** **[Selection: *NIST SP 800-38A*,** *NIST SP 800-38B, NIST SP 800-38C,* ***NIST SP 800-38D****]*
FCS_COP.1(b1)	**Cryptographic Operation (for signature generation/verification)** (for O.UPDATE VERIFICATION)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

	FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(b1)	Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [selection: *-Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],* ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits*** or greater***]***, or *-Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]*] that meets the following **[selection:** *Case: Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"* ***Case: RSA Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"*** *Case: Elliptic Curve Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"* *The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").*].
FCS_COP.1(b2)	**Cryptographic Operation (for signature generation/verification)** (for O.COMMS_PROTECTION)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys) FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(b2)	Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [**selection:** *-Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater]*, ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits, 3072 bits], or*** ***-Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits, 384bits, 521bits]***] that meets the following [**selection**:

	Case: Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard" ***Case: RSA Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"*** ***Case: Elliptic Curve Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"*** ***The TSF shall implement "NIST curves" P-256, P384 and [selection: P521****, no other curves****] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***].
FCS_COP.1(c1)	**Cryptographic operation (Hash Algorithm)** (selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)
Hierarchical to: Dependencies:	No other components. No dependencies.
FCS_COP.1.1(c1)	Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [**selection:** *SHA-1*, ***SHA-256***, *SHA-384*, *SHA-512*] that meet the following: [**ISO/IEC 10118-3:2004**].
FCS_COP.1(c2)	**Cryptographic operation (Hash Algorithm)** (for O.COMMS_PROTECTION)
Hierarchical to: Dependencies:	No other components. No dependencies.
FCS_COP.1.1(c2)	Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [**selection:** ***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].
FCS_COP.1(d)	**Cryptographic operation (AES Data Encryption/Decryption)** (for O. STORAGE_ENCRYPTION)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(d)	The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used**

	in [selection: *CBC*, *GCM*, *XTS*] mode and cryptographic key sizes [**selection:** *128 bits*, ***256 bits***] that meet the following: **AES as specified in ISO/IEC 18033-3**, [**selection: *CBC as specified in ISO/IEC 10116*, *GCM as specified in ISO/IEC 19772*, and *XTS as specified in IEEE1619***].
FCS_COP.1(f)	**Cryptographic operation (Key Encryption)** (selected from FCS_KYC_EXT.1.1)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys) FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(f)	Refinement: The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [[selection: *CBC*, *GCM*] mode**] and cryptographic key sizes [**selection:** *128 bits*, ***256 bits***] that meet the following: [**AES as specified in ISO /IEC 18033-3, [selection: *CBC as specified in ISO/IEC 10116*, *GCM as specified in ISO/IEC 19772***].
FCS_COP.1(g)	**Cryptographic Operation (for keyed-hash message authentication)** (selected with FCS_IPSEC_EXT.1.4)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys) FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(g)	Refinement: The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC**-[selection: ***SHA-1***, *SHA-224*, ***SHA-256***, ***SHA-384***, *SHA-512*], key size [assignment: *160, 256, 384*], **and message digest sizes** [**selection: *160***, *224*, ***256***, ***384***, *512*] bits that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**
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_KYC_EXT.1	**Key Chaining** (for O.STORAGE_ENCRYPTION)
Hierarchical to:	No other components.
Dependencies:	[FCS_COP.1(e) Cryptographic operation (Key Wrapping), or FCS_SMC_EXT.1 Extended: Submask Combining, or FCS_COP.1(f) Cryptographic operation (Key Encryption), or FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or FCS_COP.1(i) Cryptographic operation (Key Transport)]
FCS_KYC_EXT.1.1	The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEV or DEK;* ***intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s):*** [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1,* ***key encryption as specified in FCS_COP.1(f),*** *key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]] while maintaining an effective strength of [selection: *128 bits,* ***256 bits***].
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 [selection: *ISO/IEC 18031:2011,* ***NIST SP 800-90A***] using [selection: *Hash_DRBG (any), HMAC_DRBG (any),* ***CTR_DRBG (AES)***].

FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment:*1*] 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/IEC18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.
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 [selection: *TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] supporting the following cipher suites: 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
].

6.2.3. Class FDP: User Data Protection

FDP_ACC.1	**Subset access control** (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute-based access control
FDP_ACC.1.1	Refinement: The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **Table 12 and Table 13**.
FDP_ACF.1	**Security attribute-based access control** (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	Refinement: The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in **Table 12 and Table 13**.
FDP_ACF.1.2	Refinement: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 12 and Table 13***.

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

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

Table 12 D.USER.DOC Access Control SFP

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

Fax receive	***Operation:***	***Receive a fax and store it***	***View fax image or Release printed fax output***	***Modify image of received fax***	***Delete image of received fax***
	Fax owner	**(note 3)**		***denied***	
	U.ADMIN	**(note 4)**		***denied***	
	U.NORMAL	**(note 4)**	**denied**	**denied**	**denied**
	Unauthenticated	***(note 4)***	**denied**	**denied**	**denied**
Storage/Retrieval	***Operation:***	***Store document***	***Retrieve stored document***	***Modify stored document***	***Delete stored document***
	Job owner	**(note 1)**		***denied***	
	U.ADMIN		***(note 5)***	***denied***	***(note 5)***
	U.NORMAL		**denied**	**denied**	**denied**
	Unauthenticated	***denied***	**denied**	**denied**	**denied**

Table 13 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)**			
	U.ADMIN				
	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)**			
	U.ADMIN			***denied***	
	U.NORMAL			**denied**	**denied**
	Unauthenticated	**denied**	***denied***	**denied**	**denied**
Fax send	***Operation:***	***Create fax send job***	***View fax job status/log***	***Modify fax send job***	***Cancel fax send job***
	Job owner	**(note 2)**		***denied***	
	U.ADMIN			***denied***	

	U.NORMAL			**denied**	**denied**
	Unauthenticated	**denied**	***denied***	**denied**	**denied**
Fax receive	***Operation:***	***Create fax receive job***	***View fax receive status/log***	***Modify fax receive job***	***Cancel fax receive job***
	Fax owner	**(note 3)**		***denied***	
	U.ADMIN	**(note 4)**		***denied***	
	U.NORMAL	**(note 4)**		**denied**	**denied**
	Unauthenticated	***(note 4)***	***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, fax send, or retrieval Job.
Note 3: Job Owner of received faxes is assigned by configuration. Ownership of received faxes is assigned to a specific user.
Note 4: PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.
Note 5: Key Operator can operate the DOC/JOB of all users, while SA can operate the DOC/JOB of his/her own only.

FDP_DSK_EXT.1	**Protection of Data on Disk** (for O.STORAGE_ENCRYPTION)
Hierarchical to: Dependencies:	No other components. 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.
FDP_FXS_EXT.1	**Fax separation** (for O.FAX_NET_SEPARATION)
Hierarchical to: Dependencies:	No other components. No dependencies.
FDP_FXS_EXT.1.1	The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.
FDP_RIP.1(a)	**Subset residual information protection** (for O.IMAGE_OVERWRITE)
Hierarchical to: Dependencies:	No other components. No dependencies.
FDP_RIP.1.1(a)	Refinement: The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting** data upon the **deallocation of the resource** from the following objects: **D.USER.DOC**.

6.2.4. Class FIA: Identification and Authentication

FIA_AFL.1	**Authentication failure handling** (for O.USER_I&A)
Hierarchical to: Dependencies:	No other components. FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [selection: [assignment: *5*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] unsuccessful authentication attempts occur related to [assignment: *User authentication (with local authentication)*].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: *Identification and authentication of relevant user is inhibited until TOE is cycled.*].

FIA_ATD.1	**User attribute definition** (for O.USER_AUTHORIZATION)
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *User Identifier, User Role*].
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: [selection: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"*, [assignment: *" (space)", "", "'", "+", ",", "-", "/", ":", ";", "<", "=", ">", "?", "[", "¥", "]", "_", "`", "{", "|", "}", "~"*]]; ▪ 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 [assignment: *storing the fax data received from public telephone line*] 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 [assignment: ●] 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 [assignment: *storing the fax data received from public telephone line*] 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: [assignment: *User Identifier, User Role*].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *none*].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *none*].

6.2.5. Class FMT: Security Management

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

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

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to [selection: *determine the behavior of, disable, enable, modify the behavior of*] the functions [assignment: *List of security functions in Table 14*] to **U.ADMIN**.

Table 14 List of Security Functions

Function	Operation
User Authentication	*enable, disable*
Auditing	*enable, disable*
Trusted communications	*enable, disable, modify the behavior*
Storage Data Encryption	*enable, disable*
Overwrite Storage	*enable, disable, modify the behavior*
Firmware update	*enable, disable*
Self Test	*enable, disable*

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

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

FMT_MSA.1.1 Refinement:The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: creation]*] the security attributes [assignment: *the security attributes listed in Table 15*] to [assignment: *the roles listed in Table 15*].

Table 15 Security Attributes and Authorized Roles

Security attributes	**Operation**	**Role**
User identifier (Key Operator case)	*modify*	*Key Operator*
User identifier (General case)	*modify, delete, creation*	*U.ADMIN*
User Role (Key Operator case)	*query*	*Key Operator*
User Role (General case)	*query, modify*	*U.ADMIN*

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 [selection, choose one of: *restrictive, permissive, [assignment: none]*] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	Refinement:The TSF shall allow the [selection: *U.ADMIN,* **no role**] to specify alternative initial values to override the default values when an object or information is created.
FMT_MTD.1	**Management of TSF data** (for O.ACCESS CONTROL)
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 16.**

Table 16 Management of TSF Data

Data	Operation	Authorized Role(s)
TSF Data owned by U.NORMAL or associated with documents or jobs owned by U.NORMAL.		
U.NORMAL password	*modify*	**U.ADMIN, the owning U.NORMAL.**
TSF Data not owned by a U.NORMAL		
Key Operator password	*modify*	**U.Admin *(Key Operator)***
SA password	*modify*	**U.ADMIN**
Data on use of password entered from MFD control panel in user authentication	*query, modify*	**U.ADMIN**

Data on minimum user password length	*query, modify*	**U.ADMIN**
Data on Private Charge Print	*query, modify*	**U.ADMIN**
Data on access denial due to authentication failure	*query, modify*	**U.ADMIN**
Data on Customer Engineer operation restriction	*query, modify*	**U.ADMIN**
Data on date and time	*query, modify*	**U.ADMIN**
Data on Auto Clear	*query, modify*	**U.ADMIN**
Data on Report Print	*query, modify*	**U.ADMIN**
Software, firmware, and related configuration data		
Controller ROM, Fax ROM	*modify*	**U.ADMIN**

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

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

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *Security Management Functions listed in Table 17*].

Table 17 Security Management Functions

Management Functions	***Operation***
Registration of U.NORMAL/SA	*query, modify, delete creation*
Data on user authentication	*query, modify*
Key Operator identifier	*modify*
Key Operator password	*modify*
Data on use of password entered from MFD control panel in user authentication	*query, modify*
Data on Private Charge Print	*query, modify*
Data on trusted communications	*query, modify*
Data on date and time	*query, modify*
Data on auditing	*query, modify*
Data on storage data encryption	*query, modify*
Data on Overwrite Storage	*query, modify*

Data on Customer Engineer operation restriction	*query, modify*
Data on Self Test	*query, modify*
Data on access denial due to authentication failure	*query, modify*
Data on minimum user password length	*query, modify*
Data on Auto Clear	*query, modify*
Data on firmware update	*query, modify*
Data on Report Print	*query, modify*
Controller ROM, Fax ROM	*modify*

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.ADMIN, SA, Key Operator*), U.NORMAL**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.2.6. Class FPT: Protection of the TSF

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**.
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 **[selection:** *published hash,* ***no other functions*****]** prior to installing those updates.

6.2.7. Class FTA: TOE Access

FTA_SSL.3	**TSF-initiated termination** (for O.USER_I&A)
Hierarchical to:	No other components.

Dependencies:	No dependencies.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [assignment: *Auto Clear time for the control panel: 10 to 900 seconds* *Login timeout for the Web UI: one to 240 minutes* *There is no inactive time with printer driver*].

6.2.8. Class FTP: Trusted Paths/Channels

FTP_ITC.1	**Inter-TSF trusted channel** (for O.COMMS_PROTECTION, O.AUDIT)
Hierarchical to: Dependencies:	No other components. [FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_ITC.1.1	Refinement: The TSF shall **use [selection:** *IPsec, SSH,* ***TLS, TLS/HTTPS*****] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [selection:** *authentication server,* ***[assignment:*** *Audit Log 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 [assignment: *mail service, and audit transmission service*].
FTP_TRP.1(a)	**Trusted path (for Administrators)** (for O.COMMS_PROTECTION)
Hierarchical to: Dependencies:	No other components. [FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or

	FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_TRP.1.1(a)	Refinement: The TSF shall **use [selection, choose at least one of:** ***IPsec, SSH, TLS, TLS/HTTPS*****] to** provide a **trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.
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: Dependencies:	No other components. [FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_TRP.1.1(b)	Refinement : The TSF shall **use [selection, choose at least one of:** ***IPsec, SSH, TLS, TLS/HTTPS*****] to** provide **a trusted** communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.
FTP_TRP.1.2(b)	Refinement: The TSF shall permit [selection: ***the TSF, remote users***] to initiate communication via the trusted path
FTP_TRP.1.3(b)	Refinement: The TSF shall require the use of the trusted path for **initial user authentication and all remote user actions**.

6.3. Security Assurance Requirements

The requirements for the TOE security assurance are described in Table 18.

Table 18 Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

The rationale for choosing these security assurance requirements is that they define a minimum security baseline that is based on the anticipated threat level of the attacker, the security of the Operational Environment in which the TOE is deployed, and the relative value of the TOE itself.

6.4. Security Requirement Rationale

6.4.1. Dependencies of Security Functional Requirements

Table 19 describes the functional requirements that security functional requirements depend on and those that do not and the reason why it is not problematic even if dependencies are not satisfied.

Table 19 Dependencies of Functional Security Requirements

Functional Requirements	**Dependencies of Functional Requirements**		
Requirement and its name	**Requirement specified in PP**	**Un-fulfilled requirement and its rationale**	**Fulfilment**
FAU_GEN.1 Audit data generation	FPT_STM.1	-	OK
FAU_GEN.2 User identity association	FAU_GEN.1 FIA_UID.1	-	OK
FAU_STG_EXT.1 Extended: External audit trail storage	FAU_GEN.1 FTP_ITC.1	-	OK
FCS_CKM.1(a) Cryptographic key generation (asymmetric keys)	[FCS_COP.1(b), or FCS_COP.1(i)] FCS_CKM_EXT.4	-	OK
FAU_SAR.1 Audit review	FAU_GEN.1	-	OK
FAU_SAR.2 Restricted audit review	FAU_SAR.1	-	OK
FAU_STG.1 Protected audit trail storage	FAU_GEN.1	-	OK
FAU_STG.4 Prevention of audit data loss	FAU_STG.1	-	OK
FCS_CKM.1(b) Cryptographic key generation (symmetric keys)	[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	-	OK
FCS_CKM.4 Cryptographic key destruction	[FCS_CKM.1(a), or FCS_CKM.1(b)]	-	OK

Functional Requirements	**Dependencies of Functional Requirements**		
Requirement and its name	**Requirement specified in PP**	**Un-fulfilled requirement and its rationale**	**Fulfilment**
FCS_CKM_EXT.4 Extended: Cryptographic key material destruction	[FCS_CKM.1(a), or FCS_CKM.1(b)] FCS_CKM.4	-	OK
FCS_COP.1(a) Cryptographic operation (symmetric encryption/decryption)	FCS_CKM.1(b) FCS_CKM_EXT.4	-	OK
FCS_COP.1(b) Cryptographic operation (signature generation/verification)	FCS_CKM.1(a) FCS_CKM_EXT.4	-	OK
FCS_COP.1(c) Cryptographic operation (hash algorithm)	None	-	OK
FCS_COP.1(d) Cryptographic operation (AES data encryption/decryption)	CS_CKM.1(b) FCS_CKM_EXT.4	-	OK
FCS_COP.1(f) Cryptographic operation (key encryption)	CS_CKM.1(b) FCS_CKM_EXT.4	-	OK
FCS_COP.1(g) Cryptographic operation (for keyed-hash message authentication)	CS_CKM.1(b) FCS_CKM_EXT.4	-	OK
FCS_HTTPS_EXT.1 Extended: HTTPS selected	FCS_TLS_EXT.1	-	OK
FCS_KYC_EXT.1 Extended: Key chaining	[FCS_COP.1(e), or FCS_SMC_EXT.1, or FCS_COP.1(i), or FCS_KDF_EXT.1, and/or FCS_COP.1(f)]	-	OK
FCS_RBG_EXT.1 Extended: Cryptographic operation (random bit generation)	None		-
FCS_TLS_EXT.1 Extended: TLS selected	FCS_CKM.1(a) FCS_COP.1(a)	-	OK

Functional Requirements	**Dependencies of Functional Requirements**		
Requirement and its name	**Requirement specified in PP**	**Un-fulfilled requirement and its rationale**	**Fulfilment**
	FCS_COP.1(b) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1		
FDP_ACC.1 Subset access control	FDP_ACF.1	-	OK
FDP_ACF.1 Security attribute-based access control	FDP_ACC.1 FMT_MSA.3	-	OK
FDP_DSK_EXT.1 Extended: Protection of data on disk	FCS_COP.1(d)	-	OK
FDP_FXS_EXT.1 Extended: Fax separation	None		-
FDP_RIP.1(a) Subset residual information protection	None		-
FIA_AFL.1 Authentication failure handling	FIA_UAU.1	-	OK
FIA_ATD.1 User attribute definition	None		-
FIA_PMG_EXT.1 Extended: Password management	None		-
FIA_UAU.1 Timing of authentication	FIA_UID.1	-	OK
FIA_UAU.7 Protected authentication feedback	FIA_UAU.1	-	OK
FIA_UID.1 Timing of authentication	None		-
FIA_USB.1 User-subject binding	FIA_ATD.1	-	OK
FMT_MOF.1 Management of security functions behavior	FMT_SMF.1 FMT_SMR.1	-	OK
FMT_MSA.1	FDP_ACC.1	-	OK

Functional Requirements	**Dependencies of Functional Requirements**		
Requirement and its name	**Requirement specified in PP**	**Un-fulfilled requirement and its rationale**	**Fulfil ment**
Management of security attributes	FMT_SMF.1 FMT_SMR.1		
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 FMT_SMR.1	-	OK
FMT_MTD.1 Management of TSF data	FMT_SMF.1 FMT_SMR.1	-	OK
FMT_SMF.1 Specification of management functions	None		-
FMT_SMR.1 Security roles	FIA_UID.1	-	OK
FPT_KYP_EXT.1 Extended: Protection of key and key material	None		-
FPT_SKP_EXT.1 Extended: Protection of TSF data	None		-
FPT_STM.1 Reliable time stamps	None		-
FPT_TST_EXT.1 Extended: TSF testing	None		-
FPT_TUD_EXT.1 Extended: Trusted update	FCS_COP.1(b) FCS_COP.1(c)	-	OK
FTA_SSL.3 TSF-initiated termination	None		-
FTP_ITC.1 Inter-TSF trusted channel	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	-	OK
FTP_TRP.1(a) Trusted path (for administrators)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	-	OK
FTP_TRP.1(b) Trusted path (for non-administrators)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	-	OK

6.4.2. Security Assurance Requirements Rationale

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

7. TOE Summary Specification

This chapter describes the summary specifications of the security functions provided by the TOE.

7.1. Security Functions

Table 20 shows security functional requirements and the corresponding TOE security functions.
The security functions described in this section satisfy the TOE security functional requirements specified in section 6.1 of this ST.

Table 20 Security Functional Requirements and the Corresponding TOE Security Functions

	Security functions								
SFRs	Identification and authentication	Security audit	Access control	Security management	Trusted operation	Data encryption	Trusted communications	PSTN Fax-Network Separation	Overwrite Storage
FAU_GEN.1		✓							
FAU_GEN.2		✓							
FAU_STG_EXT.1		✓							
FAU_SAR.1		✓							
FAU_SAR.2		✓							
FAU_STG.1		✓							
FAU_STG.4		✓							
FCS_CKM.1(a)						✓			
FCS_CKM.1(b)						✓			
FCS_CKM.4						✓			
FCS_CKM_EXT.4						✓			
FCS_COP.1(a)						✓			
FCS_COP.1(b1)						✓			
FCS_COP.1(b2)						✓			
FCS_COP.1(c1)						✓			
FCS_COP.1(c2)						✓			
FCS_COP.1(d)						✓			
FCS_COP.1(f)						✓			

	Security functions								
SFRs	Identification and authentication	Security audit	Access control	Security management	Trusted operation	Data encryption	Trusted communications	PSTN Fax-Network Separation	Overwrite Storage
FCS_COP.1(g)						✓			
FCS_HTTPS_EXT.1							✓		
FCS_KYC_EXT.1						✓			
FCS_RBG_EXT.1						✓	✓		
FCS_TLS_EXT.1							✓		
FDP_ACC.1			✓						
FDP_ACF.1			✓						
FDP_DSK_EXT.1						✓			
FDP_FXS_EXT.1								✓	
FDP_RIP.1(a)									✓
FIA_AFL.1	✓								
FIA_ATD.1	✓								
FIA_PMG_EXT.1	✓								
FIA_UAU.1	✓								
FIA_UAU.7	✓								
FIA_UID.1	✓								
FIA_USB.1	✓								
FMT_MOF.1				✓					
FMT_MSA.1				✓					
FMT_MSA.3				✓					
FMT_MTD.1				✓	✓				
FMT_SMF.1				✓	✓				
FMT_SMR.1				✓					
FPT_KYP_EXT.1						✓			
FPT_SKP_EXT.1				✓					
FPT_STM.1		✓							
FPT_TST_EXT.1					✓				
FPT_TUD_EXT.1					✓				

SFRs	Security functions								
	Identification and authentication	Security audit	Access control	Security management	Trusted operation	Data encryption	Trusted communications	PSTN Fax-Network Separation	Overwrite Storage
FTA_SSL.3	✓								
FTP_ITC.1							✓		
FTP_TRP.1(a)							✓		
FTP_TRP.1(b)							✓		

7.1.1. Identification and Authentication

The identification and authentication function is the function to identify and authenticate a user by having the user enter a user ID and password from the control panel, CWIS and printer driver of the user client so that only certain authorized users are granted permissions to use the functions of the MFD.
User information registered in the MFD is used for identification and authentication.

(1) FIA_AFL.1 Authentication failure handling

The TOE authenticates users before they access the TOE. The TOE has the function to handle authentication failures when a user attempts to be authenticated. This function detects failed local authentication attempts made by the user. When the number of consecutive failed authentication attempts of the user reaches 5, which is set as the maximum allowable number of failures, the TOE does not accept an identification and authentication request of the user until the TOE is turned off and on again.

【Related TSFI】
Identification and authentication of control panel
Identification and authentication of CWIS
Printer driver
External audit server

(2) FIA_ATD.1 User attribute definition
FIA_USB.1 User-subject binding

The TOE defines a user ID and a role as attributes for each user and assign the attributes to an identified and authenticated user.

【TSFI related to FIA_ATD.1】
Management functions of control panel
Management functions of CWIS

【TSFI related to FIA_USB.1】
Identification and authentication of control panel
Identification and authentication of CWIS
External audit server

(3) FIA_PMG_EXT.1 Password Management

In the TOE, when a Key Operator's password is changed and when the password of a user authenticated by local authentication is newly created or changed, it is possible to create a password by combining the following characters.
Characters that can be used for a password:
Upper- and lower-case letters, numbers, and the following special characters:
"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "(space)", """, "'", "+", ",", "-", "/", ":", ";", "<", "=", ">", "?", "[", "¥", "]", "_", "`", "{", "|", "}", "~"
A system administrator can set the required minimum length of the password to a number between 0 to 63. Based on this setting, the TOE can set a lower limit of the password length to 15.

【Related TSFI】
Management functions of control panel
Management functions of CWIS

(4) FIA_UAU.1 Timing of authentication
FIA_UID.1 Timing of identification

The TOE supports local authentication as the user identification and authentication method.
There are four types of interfaces that require user identification and authentication: the control panel, web browser of the user client, printer driver, and audit server.
The TOE prompts a user to enter his/her ID and password via a web browser of the user client or the control panel before permitting him/her to operate the MFD function. The entered user ID and password are verified against the user data registered in the TOE.
The audit server prepares a PowerShell script in which system administrators' IDs and passwords are written, and the script is executed on the audit server. Executing the script sends the IDs and passwords from the audit server to the TOE via https, and the TOE performs identification and authentication using the received IDs and passwords.
When Private Print is performed, identification and authentication are performed based on the ID and password assigned to the print data sent from the client computer.

The identification (FIA_UID.1) and authentication (FIA_UAU.1) are simultaneously performed, and the operation on the TOE is allowed only when both identification and authentication succeed.
When receiving fax data via the public telephone line, the TOE receives the fax data without user identification and authentication.

【Related TSFI】
Identification and authentication of control panel
Identification and authentication of CWIS
Printer driver
External audit server
Public phone line

(5) FIA_UAU.7 Protected authentication feedback

The TOE provides the function to display the same number of bullets (●) as the password characters entered on the control panel or web browser in order to hide the password at the time of user authentication.

【Related TSFI】
Identification and authentication of control panel
Identification and authentication of CWIS

(6) FTA_SSL.3 TSF-initiated termination

The TOE clears the login information (authentication session) and prompts a user to re-authenticate if CWIS has not been accessed from a web browser for a specified period of time (settable from one to 240 mins).
In addition, when there is no operation from the control panel for a specified period of time (the settable time ranges from 10 to 900 seconds), the setting on the control panel is cleared and the screen returns to the authentication screen.
The session with the printer driver is not retained. The session ends immediately after a print request is processed.

【Related TSFI】
Identification and authentication of control panel
Identification and authentication of CWIS

7.1.2. Security Audit

The security audit function offers a means to track and log the activities of all TOE users (when and who carried out which actions) and important events (device failure, configuration change, user operation, etc.) according to the Security Audit Log setting configured by a system administrator in system administrator mode.

(1) FAU_GEN.1 Audit data generation
FAU_GEN.2 User identity association

The TOE records auditable events shown in Table 21, such as job completion, failed user identification and authentication attempts, and use of security management functions by identified and authenticated users, in the audit log. The date and time when the event occurred, the type of the event, the user who caused the event (if known), and the result of the event are recorded in the audit data of each event.
When the TOE records a defined auditable event in the audit log file, the TOE associates the event with the identification information of the user who caused the event.

【Related TSFI】
Identification and authentication of control panel
Identification and authentication of CWIS
Printer driver
Management functions of control panel
Management functions of CWIS
Power button
Copy, print, scan, fax, scanned document storage to Mailbox, and document retrieval functions of control panel
Job management and log display functions of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server
Firmware update function of CWIS
Public phone line

Table 21 Details of Security Audit Log

Auditable Events	**Names of auditable events to be logged**	**Description**
Start-up and shutdown of the audit functions	System Status/ Started normally (cold boot), System Status/ Started normally (warm boot), Shutdown requested	
Job completion	Job Status/ Completed, Job Status/ Canceled by User	Print
		Copy
		Scan
		Fax
		Mailbox **[**"Mailbox" means a storage and retrieval job.**]**

Unsuccessful User authentication Unsuccessful User identification (control panel, CWIS, and audit server)	Login/ Failed (Invalid UserID), Login/ Failed (Invalid Password)	
Unsuccessful User authentication Unsuccessful User identification (printer driver)	Job Status/ Print /Aborted	
Use of management functions	Device Settings/ View Security Setting	
	Device Settings/ Change Security Setting	
	Device Settings/ Switch Authentication Mode	
	Device Settings/ Edit User [“ID”, “Password”, and “Name” are recorded as modified attributes.]	
	Device Settings/ Add User	
	Device Settings/ Delete User	
	Device Config/ Software	
	Audit Policy/ Audit Log/ Enable, Audit Policy/ Audit Log/ Disable	
Modification to the group of Users that are part of a role	Device Settings/ Edit User [When “Role” attribute is modified, the modification is recorded.]	
Changes to the time	Device Settings / Adjust Time	
Failure to establish session (TLS)	Communication / Trusted Communication	Failed [Protocol, destination and the reason of failure are recorded]

(2) FAU_SAR.1 Audit review

After logging in to the CWIS, the system administrator can read all the information recorded in the security audit log data by using the CWIS.

Security audit log data is downloaded as a tab-delimited text file. When downloading the security audit log data, TLS communication must be enabled.

【Related TSFI】

Management functions of CWIS

(3) FAU_SAR.2 Restricted audit review

The function to read the security audit log data is restricted to the authenticated system administrator. Also, the security audit log data can be accessed only from the web browser and can not be accessed from the control panel.

【Related TSFI】
Management functions of CWIS

(4) FAU_STG.1 Protected audit trail storage

Access to the security audit log data is for reading only, there is no delete or modify function. This protects the security audit log data from unauthenticated deletion and modification.

【Related TSFI】
Management functions of CWIS

(5) FAU_STG.4 Prevention of audit data loss

The audit log target events are stored in the storage device in the TOE internally. The storage device can store up to 15,000 events. When the security audit log data becomes full, the oldest recorded audit data is overwritten and new audit data is recorded without loss.

【Related TSFI】
Identification and authentication of control panel
Identification and authentication of CWIS
Printer driver
Management functions of control panel
Management functions of CWIS
Power button
Copy, print, scan, scanned document storage to Mailbox, fax, and document retrieval functions of control panel
Job management and log display functions of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server
Firmware update function of CWIS
Public phone line

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

The security audit log data is sent to an external audit server as a tab-delimited text file by the request from the server. When an external audit server requests the TOE to send the security audit log data, the TOE sends all stored data to the server. When sending to an external audit server, the data is encrypted with TLS/HTTPS.
Only authenticated system administrators can retrieve security audit log data.
The maximum number of audit log target events temporarily stored in the TOE internally and the behavior when the events exceed the maximum number are described in (5) FAU_STG.4.

【Related TSFI】
External audit server

(7) FPT_STM.1 Reliable time stamps

The TOE provides the function to issue the time stamp using TOE's clock function when the defined auditable event is recorded in the audit log file.
As specified in FMT_MTD.1, only system administrators can change the clock setting.

【Related TSFI】
Follow the related TSFI of FAU_GEN.1, FAU_GEN.2

7.1.3. Access Control

Only the authenticated and identified user can use the following functions. Available functions depend on the interface that accesses the TSF.

a) Functions controlled by the MFD control panel
Copy, fax (send), scan, document storage and retrieval, print (This print function requires the Accounting System preset on printer driver. A user must be authenticated on the control panel.), device condition display, job status and log display, and referring to / changing the TOE setting data (system administrators only)

b) Functions controlled by CWIS
Device condition display, job status and log display, function to retrieve document data from Mailbox, and referring to / changing the TOE setting data (system administrators only), and firmware update function (only system administrator)

c) Functions that use the printer driver of the user client
When a user sends a print request from the printer driver of the user's client in which the Accounting System is preset, the MFD decomposes the received data into bitmap data and stores the data in the internal repository as private print according to the user ID if the identification and authentication are successful.

(1) FDP_ACC.1 Subset access control
FDP_ACF.1 Security attribute based access control

The TOE controls access to the jobs and document data of each basic function in accordance with Tables 12 and 13. For the notes in brackets at the ends of the following sentences, refer to the notes of Tables 12 and 13.
The user who started each function is assigned as the owner of the job and document data of the function and only the owner or system administrators can access the job and document data. However, only system administrators can access the data of a fax that is being received and the data that is being transmitted from the client computer.
Regarding the print function, a user ID, which will be used to identify the user of the function, is included in the print data sent by the client computer. The owner of the print job is identified with the user ID (note 1).
Regarding scan, copy, and fax send functions' jobs, the user associated with the user ID that is used to log in on the control panel is assigned as the job owner (note 2).
Regarding fax jobs that are in progress, system administrators are assigned as the job owners because the user who started the fax send feature cannot be identified. (note 3)
Regarding the stored data of a received fax, the user ID associated with the Mailbox that stores the data is assigned as the owner (note 3).
Because Jobs and data of received faxes are sent from outside of the TOE, no TOE user can create jobs or data of received faxes. (note 4)
The document storage and retrieval function enable the function to store/retrieve scanned documents or fax received documents to/from the Mailbox. Regarding the scan function, the user must be logged in beforehand. When a user stores scanned documents in a Mailbox, the Key Operator can select a Mailbox from all Mailboxes, while a general user and SA can only select the user's own Mailbox. After selecting the Mailbox to store scanned documents, the user scans the documents. The user who owns the selected Mailbox becomes the owner of the scanned documents (note 1). Only the owner of the data stored in the Mailbox or the Key Operator can retrieve, print (and select the number of copies and the paper size) and delete the stored data. Although SAs are included in system administrators, they cannot access the data in the Mailboxes of other users (note 5). The print, scan, copy, fax send, fax receive, and the document storage and retrieval functions do not provide the function of editing document data.
The function to modify the scan jobs of scan, fax send, and fax receive are not provided.

【Related TSFI】
Printer driver
Copy, print, scan, scanned document storage to Mailbox, fax and document retrieval functions of control panel
Function of control panel to display the job status and log
Function of CWIS to display the job status and log
Function of CWIS to retrieve document data from Mailbox
Public phone line

7.1.4. Security management

(1) FMT_MOF.1 Management of security functions behavior
FMT_MTD.1 Management of TSF data
FMT_SMF.1 Specification of Management Functions
FMT_MSA.1 Management of security attributes
FMT_MSA.3 Static attribute initialization
FMT_SMR.1 Security roles

The TOE provides identified and authenticated system administrators with user interfaces to refer to and change settings of security management functions shown in Table 22 that are related to the TOE security functions and to customize detailed settings of each function.
Identified and authenticated general users can only change their own passwords.
As shown above, the required security management functions are satisfied.
As in Table 12 and Table 13, the TOE sets the ID of the user who started each basic function as the default value of the ID of the owner of the job and document data of each function. For details, refer to "7.1.3. Access Control (1) FDP_ACC.1 Subset access control FDP_ACF.1 Security attribute based access control."
The TOE associates the roles of the Key Operator, SA, system administrator, and general user to the legitimate users and maintains the association.
In the TOE, the default value of the user role, which is a security attribute, is the general user.

【TSFI related to FMT_MOF.1,FMT_MSA.1, andFMT_SMR.1】
Management functions of control panel
Management functions of CWIS
【TSFI related to FMT_MTD.1 andFMT_SMF.1】
Management functions of control panel
Management functions of CWIS
Firmware update function of CWIS
【TSFI related to FMT_MSA.3】
Printer driver
Management functions of control panel
Management functions of CWIS
Copy, scan, and scanned document storage to Mailbox, and fax functions of control panel
Public phone line

Table 22 Security management functions and their operationable UIs

Security management item	Control panel	CWIS
Refer to the setting of Overwrite Storage, enable/disable it, and set the number of passes (overwrite procedure)	✓	✓
Refer to the setting of Storage Data Encryption and enable/disable it	✓	-

Refer to the setting of the use of password entered from MFD control panel in user authentication and enable/disable it	✓	-
Refer to the setting of access denial due to authentication failure of the user, enable/disable it, and set the allowable number of failures	✓	✓
Set the ID and the password of the Key Operator (Only the Key Operator is privileged.)	✓	✓
Refer to the setting of the ID of a user and change the ID and password Refer to the assigned role of the user and set SA or general user as the role	✓	✓
Refer to and set the minimum password length	✓	✓
Refer to the setting of communication data encryption, enable/disable it, and configured the detailed settings.	✓	✓
Refer to the setting of TLS certificate and create/update the certificate	-	✓
Refer to the setting of User Authentication and enable/disable Local Authentication	✓	✓
Refer to the setting of PrivatePrint and configure the settings of store/print	✓	-
Refer to and set date and time	✓	-
Refer to the setting of Self Test and enable/disable it	✓	✓
Refer to the setting of firmware update and enable/disable it	✓	✓
Refer to and set Auto Clear of Control Panel and CWIS	✓	✓
Refer to the setting of Report Print and select whether to allow only the system administrators / all users to use the function	✓	-
Refer to and configure the setting of Customer Engineer Operation Restriction (enable/disable the function and set password for maintenance)	✓	✓
Refer to the setting of the security audit function and enable/disable it (When enabled, the security audit log data can be sent to the audit server as a tab-separated text file.)	-	✓

(2) FPT_SKP_EXT.1 Protection of TSF Data

The TOE stores a KEK (Key Encryption Key) in plaintext in NVRAM2, but the TOE does not provide an interface to read the KEK to any users. The circuit board which NVRAM2 is soldered to is not for storage.

A DEK (Data Encryption Key) is encrypted with KEK in AES-CBC and is stored in NVRAM1 and HDD. The one in HDD is a backup.

When the TOE is turned on, the encrypted DEK stored in NVRAM1 is decrypted with a KEK stored in NVRAM2. While the TOE is in operation, the DEK is stored in DRAM in plaintext. The TOE does not provide an interface to read the plaintext DEK stored in DRAM to any users. The plaintext DEK stored in DRAM is destroyed when the TOE is turned off.

Certificates with secret keys used for TLS communications, etc. are encrypted with the mechanism described in 7.1.6 (15) and stored in the NVRAM1. The interface to read the secret keys is not provided to any users.
The TLS session key and TLS EC Diffie-Hellman secret key used for communication are stored in the DRAM in plaintext, but the interface to read the plaintext session keys stored in the DRAM is not provided to any users. The plaintext session key is destroyed when the TOE is turned off.

【Related TSFI】
None

7.1.5. Trusted Operation

(1) FPT_TST_EXT.1 TSF testing

The TSF consists of two firmware: Controller ROM and Fax ROM. Verification of the integrity of these two firmware guarantees the proper operation of the TSF.
When the TOE is turned on, Controller ROM and Fax ROM respectively calculate 4 bytes and 2 bytes checksums to verify whether the checksums match the specified value. When an error occurs, an error message is displayed on the control panel, and the TOE cancels the startup. The TOE operates health tests described in [1]11.3 on the DRBG. When the test is failed, the TOE displays an error message on the control panel and cancels the startup. The specifications of the DRBG is described in 7.1.6.

【Related TSFI】
Power button

(2) FPT_TUD_EXT.1 Trusted Update
FMT_MTD.1 Management of TSF data
FMT_SMF.1 Specification of Management Functions

The system administrators can see the current version of the firmware that configures the TOE on the control panel by operating it or on paper by printing the configuration report.
Only identified and authenticated system administrators can update the firmware by sending a binary file that contains Controller ROM and Fax ROM to the TOE from the web browser of a system administrator's client computer.
When the TOE receives a binary file that contains firmware sent from the web browser of a system administrator's client computer, the TOE verifies the digital signature attached to the binary file. When the verification fails, the update is cancelled, an error message is displayed ont the control panel, and the TOE stops. The digital signature attached to the binary file is a RSASSA-PKCS1-v1.5 digital signature that is made by hashing the binary file with SHA-256 and encrypting the hash value with a 2048-bit secret key. Therefore, in order to verify the digital signature, 1) decrypt the digital signature attached to the binary file with the RSA public key for firmware signature verification, 2) hash the binary

file with SHA-256, and 3) compare the decrypted value and the hash value. When the two values are the same, verification is successful and if not, verification is failed.

【TSFI related to FPT_TUD_EXT.1】
Function of control panel to confirm the firmware version
Firmware update function of CWIS
【TSFI related to FMT_MTD.1 and FMT_SMF.1】
Management functions of control panel
Management functions of CWIS
Firmware update function of CWIS

7.1.6. Data Encryption

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

An elliptic curve key described in [2] is used as the asymmetric key for the key establishment (EC Diffie-Hellman) in TLS encrypted communication. Methods to generate an elliptic curve key shall follow [3] 5.6.1.2.2 and [2] Appendix B.4.2. TLS EC Diffie-Hellman secret key is a random number generated by AES-256 CTR DRBG described in (14) seeded with values generated by Linux /dev/random. Supported elliptic curves are P-256, P-384, and P-521 as described in [2] Appendix D, and the elliptic curve to be used is decided in TLS negotiation.

The TOE uses an elliptic curve key described in [2] or an RSA key described in [4] as the asymmetric key for the TLS server certificate. These asymmetric keys are generated on the user request from CWIS. Methods to generate an elliptic curve key shall follow [3] 5.6.1.2.2 and [2] Appendix B.4.2. Methods to generate an RSA key shall follow [4] 6.3.1.3. The prime number used in the procedure shall be generated following [2] B.3.3. Supported elliptic curves are P-256, P-384, and P-521 as described in [2] Appendix D, and supported RSA key sizes are 2048-bit and 3072-bit. The user selects one and requests to generate a key on CWIS. AES-256 CTR DRBG described in (14) is used to generate random probable primes.

The TOE does not make any changes to the above key generation methods and does not use any other methods.

【Related TSFI】
Identification and authentication of CWIS
Printer driver
Management functions of CWIS
Scan function of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server

Firmware update function of CWIS

(2) FCS_CKM.1(b) Cryptographic Key Generation (symmetric keys)

The TOE uses random numbers that consist of arbitrary number of bits for the DEK and the session keys for trusted communications. Specifically, a 256-bit number for the DEK, a 256-bit number for the KEK to encrypt the DEK, a 128 to 256-bit number (depends on the encryption method decided in the negotiation) for the master key of TLS session keys are generated. For random number generation, AES-256 CTR DRBG described in (14) is used. The DRBG is called when the key chain described in (12) is generated and when the TLS communication session starts.

【Related TSFI】
Identification and authentication of CWIS
Printer driver
Management functions of CWIS
Power button
Scan function of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server
Firmware update function of CWIS

(3) FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4 Cryptographic Key Material Destruction

The TOE destroys plaintext keys and key materials when they are no longer needed (*). Table 23 shows keys and key materials that are stored in the TOE in plaintext and how they are destroyed. The values of these keys and materials are copied to the working memory of RAM and used when an encryption is performed. The copied data on RAM is deleted when the TOE is turned off because it is no longer needed.

(*) The DEK is stored in NVRAM1 and HDD, but it is not destroyed because it is encrypted as described in (10). The asymmetric key for TLS server certificate described in (1) is stored in the NVRAM1, but it is not destroyed because it is encrypted with the mechanism described in (15). The public key used for the verification of firmware signature is not destroyed because it is not classified as any of the following: secret key, private cryptographic key, or cryptographic critical security parameter.

【Related TSFI】
Management functions of control panel
Power button

Table 23 Methods to destroy keys and key material stored in plaintext

Key type	Storage	Destruction method and reason
KEK (Key Encryption Key)	NVRAM2	Overwritten once with the random value generated using DRBG described in (14) when restore to factory settings is requested from the administrator menu on the control panel. Restore to factory settings means destroying all data on the disk and since it is not necessary to decrypt the target partition with the same encryption key after destroying the data, DEK and KEK are not required.
TLS session key	RAM (volatile)	Destroyed when the TOE is turned off. Since the TOE closes a valid TLS session when it is powered off, TLS session key and TLS EC Diffie-Hellman secret key are not needed.
TLS EC Diffie-Hellman secret key		

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

The TOE supports AES-CBC described in [5] and AES-GCM (128-bit and 256-bit) described in [6] for the symmetric encryption/decryption of TLS. AES follows [7].

【Related TSFI】
Identification and authentication of CWIS
Printer driver
Management functions of CWIS
Scan function of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server
Firmware update function of CWIS

(5) FCS_COP.1(b1) Cryptographic Operation (for signature generation/verification)

The TOE supports RSA digital signature described in [2] for the verification of the authenticity of the firmware update. The key size is 2048-bit. The format of the signature follows RSASSA-PKCS1-v1.5 described in [2] 5.5 (f).

【Related TSFI】
Firmware update function of CWIS

(6) FCS_COP.1(b2) Cryptographic Operation (for signature generation/verification)

When verifying the target of TLS communication and digital signature generation/verification, the TOE generates RSA digital signatures and elliptic curve digital signatures described in [2] and verifies with them. Supported RSA key sizes are 2048-bit

and 3072-bit. Supported NIST elliptic curves are P256, P384, and P521. The format of the RSA digital signature follows RSASSA-PKCS1-v1.5 described in [2] 5.5 (f). The methods of generation and verification of the elliptic curve digital signature follows [2] 6.4. For these, the signature methods to be used are determined respectively by negotiation with the communication partner during TLS communication, and by the user's specification at the time of digital signature generation.

【Related TSFI】
Management functions of CWIS
Scan function of control panel

(7) FCS_COP.1(c1) Cryptographic operation (Hash Algorithm)

The TOE uses SHA-256 for the hash calculation of firmware update image data when verifying the authenticity of the firmware update. The TOE compares the SHA-256 hash value and the value of the signature decrypted with RSA to verify the signature. The hash algorithm follows [8].

【Related TSFI】
Firmware update function of CWIS

(8) FCS_COP.1(c2) Cryptographic operation (Hash Algorithm)

The TOE supports SHA1/SHA256/SHA384 for the hash calculation of keyed-hash message authentication method described in (11). The hash algorithm used for communication is determined by negotiation with the communication partner. In addition, the TOE supports SHA256/SHA384/SHA512 for hash calculation for digital signature generation/verification, and the hash algorithm to be used determined by user's specification at the time of signature generation.
The hash calculation of keyed-hash message authentication method in TLS and the hash calculation of digital signature generation/verification are independent and can be freely combined.

【Related TSFI】
Identification and authentication of CWIS
Printer driver
Management functions of CWIS
Scan function of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server
Firmware update function of CWIS

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

The TOE supports AES described in [9] as the encryption method of the storage encryption and supports CBC described in [10] as the block cipher mode. The key size is 256-bit. The sector number of the storage and the DEK are used to calculate the IV.

【Related TSFI】
Printer Driver
Copy, print, scan, scanned document storage to Mailbox, fax, and document retrieval functions of control panel
Job status and log display of control panel
Function of CWIS to retrieve document data from Mailbox
Public phone line

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

As described in (12), the TOE encrypts DEK (256-bit) using AES described in [9]. The key size is 256-bit. Supported block cipher mode is CBC described in [10]. IV is a random number generated by AES-256 CTR DRBG described in (14).
As described in (12), the TOE encrypts DEK (256 bit) when the TOE is turned on for the first time without DEK chain.

【Related TSFI】
Power button

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

The TOE supports the following for the keyed-hash message authentication of TLS.

- Key size (bit): 160, 256, and 384
- Hash: SHA-1, SHA-256, and SHA-384
- Message digest size (bit): 160, 256, and 384

The hash algorithm follows [11], and the keyed-hash message authentication algorithm (HMAC) follows [12].

【Related TSFI】
Identification and authentication of CWIS
Printer driver
Management functions of CWIS
Scan function of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server
Firmware update function of CWIS

(12) FCS_KYC_EXT.1 Key Chaining

In the TOE, the DEK and the KEK, which encrypts the DEK, are in a key chain. When the TOE is turned on without DEK chain (more specifically, when the TOE is turned on for the

first time in the factory, or when the TOE is turned on for the first time after the operation to restore factory settings is performed from the system administrator menu on the control panel), the TOE generates the DEK and KEK using DRBG described in (14). The DEK is encrypted with KEK as described in (10) and stored in NVRAM1 and HDD, and the KEK is stored in NVRAM2 in plaintext. When the TOE is turned on subsequently, the TOE decrypts the encrypted DEK stored in NVRAM1 with the KEK retrieved from NVRAM2 as described in (10). The key size of both DEK and KEK is 256-bit. As described in (14), DRBG supplies sufficient entropy, so the strength of both DEK and KEK is 256-bit, which means that the 256-bit strength is maintained in the key chain.

【Related TSFI】
Power button

(13) FPT_KYP_EXT.1 Protection of Key and Key Material

As described in (12), when the TOE is turned on for the first time without DEK chain, the TOE generates a DEK and a KEK using DRBG described later, stores the DEK encrypted with KEK in NVRAM1 and HDD, and stores the KEK in NVRAM2 in plaintext. The DEK and KEK are not stored in other storage. NVRAM2 is not a Field-Replaceable Nonvolatile Storage Device, so plaintext keys that are part of the keychain specified by (12) is not stored in any Field-Replaceable Nonvolatile Storage Device.

【Related TSFI】
Power button

(14) FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

For random number generation, the TOE uses AES-256 CTR DRBG that follows [1]10.2.1. This DRBG has derivation function and reseed function, but does not have prediction resistance function. It uses a random number generated by Linux kernel /dev/random as the seed. Linux Random Number Generator (LRNG), which provides /dev/random, and the read noise of the clock counter, which is input in LRNG, are included in the entropy pool of DRBG. The noise is created by a software so that the clock counter reads at random timings. DRBG uses the seed provided by /dev/random as the entropy input and nonce, but the amount of entropy is more than 256-bit × 1.5, which is sufficient according to [1] 8.6.7.
The TOE generates the DEK and the master key of TLS session keys using the DRBG.
As described in (12), the DRGB is activated in order to generate the DEK when TOE is turned on for the first time without DEK chain.

【Related TSFI】
Identification and authentication of CWIS
Printer driver
Management functions of CWIS
Power button

Scan function of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server
Firmware update function of CWIS

(15) FDP_DSK_EXT.1 Protection of Data on Disk

The TOE encrypts/decrypts each data block in the storage device.
More precisely, for the storage device partition that is to be encrypted, the TOE applies data decryption/encryption through the read/write operation of a file or metadata, and reads/writes data blocks from/to that partition.
Encryption method follows FCS_COP.1(d). The storage devices containing the encryption target partition are NVRAM1 and HDD, both of which are field-replaceable. There are no field-replaceable devices except for the NVRAM1 and HDD.
After Storage Data Encryption is enabled by the administrator, the encryption/decryption described above starts to be performed when the TOE is turned on for the first time. As described in (12), the DEK to be used for encryption/decryption is generated when the TOE is turned on without an cryptographic key chain.
All plaintext user data and plaintext secret TSF data are encrypted because they are written in the partitions to be encrypted on the NVRAM1 and HDD. The partitions not to be encrypted on the NVRAM1 and HDD store only program images, control parameters, and the DEK encrypted with KEK in the method specified in (10). Plaintext user document data and plaintext secret TSF data is not stored in those partitions. As described in (12), the DEK is encrypted when the TOE is turned on without a cryptographic key chain.
NVRAM2, which stores the plaintext KEK, is not a field-replaceable storage device.

【Related TSFI】
Printer driver
Management functions of CWIS
Power button
Copy, print, scan, scanned document storage to Mailbox, fax, and document retrieval functions of control panel
Job status and log display of control panel
Function of CWIS to retrieve document data from Mailbox
Public phone line

7.1.7. Trusted Communications

(1) FCS_HTTPS_EXT.1 HTTPS selected

There is a setting that forces a secure channel using HTTPS for all communication traffic of the TOE with the web browser and audit server. Only system administrators can change this setting, and it is performed on CWIS. The specifications of HTTPS follow [13].
When the TOE receives a request to connect to CWIS from the web browser of a client

computer, the TOE and the client computer establish the TLS negotiation and start HTTPS communication. Identification, authentication, and all remote operation on the TOE through CWIS of the client computer are performed via HTTPS communication. When the audit server requests to retrieve the security audit log data, the TOE sends the data to the audit server via HTTPS communication.

【Related TSFI】
Identification and authentication of CWIS
Management functions of CWIS
Function of CWIS to display the JOB status and log
Function to retrieve document data from Mailbox of CWIS
External audit server
Firmware update function of CWIS

(2) FCS_TLS_EXT.1 TLS selected

The supported TLS communication is TLS 1.2 described in [14].
The cipher suite to be used in the TLS communication is negotiated while the client and server are connected with TLS. In TLS communication, the TOE can be a client or a server depending on the function in operation. For example, the TOE acts as a server when accessing CWIS. The TOE acts as a client when sending scanned documents via email.
The TOE selects an appropriate cipher suite that the TOE supports from the cipher suites suggested by the client. Cipher suites supported by the TOE are as follows:

- 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_SHA
- TLS_ECDHE_RSA_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_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- 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

【Related TSFI】
Identification and authentication of CWIS
Printer driver
Management functions of CWIS

Scan function of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
External audit server
Firmware update function of CWIS

(3) FTP_ITC.1 Inter-TSF trusted channel

The TOE supports the following trusted communication protocols for the communication of the TOE with the audit server and the mail server. This ensures identification of the end points and protection of the channel data from disclosure and modification.

- Audit server: TLS/HTTPS
- Mail server: TLS

【Related TSFI】
Scan function of control panel
External audit server

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

The TOE supports the following trusted communication protocols for each interface to access the TOE from the remote computers of system administrators. This ensures identification of the TOE's end points and protection of the channel data from disclosure and modification.

- CWIS: TLS/HTTPS

【Related TSFI】
Identification and authentication of CWIS
Management functions of CWIS
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox
Firmware update function of CWIS

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

The TOE supports the following trusted communication protocols for each interface to access the TOE from the remote computers of non-administrators. This ensures identification of the TOE's end points and protection of the channel data from disclosure and modification.

- CWIS: TLS/HTTPS
- Printing with the printer driver: TLS

【Related TSFI】
Identification and authentication of CWIS
Printer driver
Function of CWIS to display the JOB status and log

Function of CWIS to retrieve document data from Mailbox

7.1.8. PSTN Fax-Network Separation

(1) FDP_FXS_EXT.1 Fax separation

The TOE is equipped with a fax modem function, which enables the TOE to send/receive fax data through the public phone line.
The only supported protocol is ITU-T G3 mode.
Only the fax documents of the user are allowed to be sent/received with the fax interface.
The TOE is not equipped with a data modem function, so external data communication commands cannot be received, which means the TOE cannot be accessed by unauthorized means from the fax line. Also, the TOE does not offer the function to deliver data between the public phone line and the internal network, so the data received through the public phone line is not sent to the internal network.

【Related TSFI】
Public phone line

7.1.9. Overwrite Storage

(2) FDP_RIP.1(a) Subset residual information protection

When the Overwrite Storage is enabled to be conducted after each job by a system administrator, the TOE overwrites the used document data stored in the internal HDD after each job of copy, print, scan, and fax is finished.
The document data used by the document storage function is deleted when an operation to print, retrieve or delete the data from mailbox is carried out. After that, the TOE overwrites the data.
Overwrite Storage has two options: one pass overwrite procedure (overwrite with zero) and three pass overwrite procedure (overwrite with zero / one / random number and verification). However, when the data encryption function is enabled, the data for overwrite (zero / one / random number) to be physically written to the storage is encrypted. A list of used document data to be overwritten and deleted is on the internal HDD, and the TOE checks the list when it is turned on. If used document data that has not been deleted is found on the list, Overwrite Storage is performed.

【Related TSFI】
Power button
Copy, Print, Scan, fax, and document data retrieval functions of control panel
Job status and log display of control panel
Function of CWIS to display the JOB status and log
Function of CWIS to retrieve document data from Mailbox

8. ACRONYMS AND TERMINOLOGY

8.1. Acronyms

The following acronyms are used in this ST:

Acronym	Definition
CC	Common Criteria
CWIS	CentreWare Internet Services
DRAM	Dynamic Random Access Memory
FIPS PUB	Federal Information Processing Standard publication
IIT	Image Input Terminal
MFD	Multi Function Device
NVRAM	Non Volatile Random Access Memory
PDL	Page Description Language
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2. Terminology

The following terms are used in this ST:

Term	Definition
Destruction	Destruction is to delete the target so that the location of the target cannot be traced from the file system and volatile memory.
KEK	Abbreviation of Key Encryption Key. In this ST, KEK is a cryptographic key to encrypt the DEK.
DEK	Abbreviation of Data Encryption Key. In this ST, DEK is a cryptographic key for storage.
Flash memory	SD or eMMC.
Web UI	A service that allows users to control the TOE through the web browser of the user client.
Mailbox	A location to store scanned documents, received fax documents. Computers on the network can retrieve the stored documents from the Mailbox.
Private Print (Private Charge Print)	A print function that temporarily stores bitmap data (decomposed print data) in the storage of the MFD and then print out in accordance with the authenticated user's instruction from the control panel.

Used document data	The remaining data in the storage of the MFD after deletion. After a document stored in the storage is used, only its file is deleted, and the data inside remains.
Document data	A collective term for all the data, including image data, transmitted across the MFD when any of copy, print, scan, fax, or document storage functions is used by a general user (U.NORMAL) or an SA.
Scanned document	The document data converted into digital format by "Scan" function. This TOE has the function to send a scanned document to a mailserver and to store it in the Mailbox by "Document storage and retrieval" function.
Fax received document	The digital document data received by fax function and handled in this TOE. With this TOE, the received fax data can be stored in a preset Mailbox by the setting at the time of installation.
Security audit log data	The chronologically recorded data of auditable events including important events of the TOE, such as device failure, configuration change, and user operation. These events are traced and recorded based on when and who operated what function.
User role	A role assigned to an identified and authenticated user. The TOE defines the Key Operator role, SA role, and general user role.
Key Operator role	The authority required for the Key Operator to use the TOE.
SA role	The authority required for an SA to use the TOE.
U.NORMAL role	The authority required for a general user (U.NORMAL) to use the TOE.
User identifier	Information to identify users. User ID.
Key Operator identifier	A user ID with the Key Operator role.
Key Operator	An authorized user who maintains the MFD and performs settings of the security functions of the TOE.
SA	An authorized user who maintains the MFD and performs settings of the security functions of the TOE. An SA account is created by the Key Operator or an SA who is already registered.
U.ADMIN	A collective term for Key Operator and SA.
CWIS (CentreWare Internet Services)	CWIS is a service that allows the user to access the TOE via the web browser of the client computer. The user can confirm the status of the TOE, change settings of the TOE, and request retrieval and printing of documents. CWIS operates on a standard web browser of Windows.
User authentication	A function to identify the user before he/she uses each TOE function so that the TOE can limit the access to the TOE functions. When the remote authentication option is installed, user authentication supports two modes (local authentication and remote authentication). The TOE uses local authentication.
Local Authentication	A mode to perform user authentication of the TOE using the user information registered in the MFD.
Remote Authentication	A mode to perform user authentication of the TOE using the user information registered in the external authentication server.

Storage data encryption	A function to encrypt the storage that stores some of the assets under protection.
Decompose function	A function to analyze the data written in PDL and convert the data into bitmap data.
Decompose	The action of analyzing the data written in PDL and converting the data into bitmap data by using the decompose function.
System administrator mode	An operation mode that enables a system administrator to refer to and rewrite TOE device operation settings and security function settings in order to adjust those settings in accordance with the operational environment. System administrator mode is distinguished from the operation mode that enables a general user to use the MFD functions.
Auto Clear	A function to automatically log out after a specified period of time passes without any operations performed on the control panel or CWIS.
Customer Engineer	Customer service engineer, an engineer who maintains and repairs the MFD.
Attacker	A person who accesses the TOE or protected property by unauthorized means. Includes users who attempt access by disguising themselves as authenticated users.
Control panel	A panel on which buttons, lamps, and a touch-screen display, which are necessary for MFD operations, are arranged.
General user client	A client for a general user.
System administrator client	A client for a system administrator. A system administrator can refer to and change the TOE setting data of the MFD via web browser.
Printer driver	A software to convert the data on a general user client into print data written in page description language (PDL), a readable format for MFD. Used on the user client.
Print data	The data written in PDL, a readable format for MFD. Print data is converted into bitmap data by the decompose function of the TOE.
Bitmap data	The decomposed data of the data read by the copy function and the print data transmitted sent by the print function from a user client to MFD. Bitmap data is stored to the storage after being compressed in a unique process.
Original document	Texts, images and photos to be read on IIT by the copy function.
TOE setting data	The data created by the TOE or for the TOE and may affect the TOE security functions. Included in the TSF data.
Cryptographic key	256-bit data which is automatically generated. When document data is stored to the storage device, it is encrypted with the cryptographic key.
Network	A general term to indicate both external and internal networks.
External network	The network which cannot be managed by the organization that manages the TOE. This does not include the internal network.

Internal network	Channels between the MFD and the trusted remote servers and client computers. The channels are located in the network of the organization that owns the TOE. The network is protected from the security risks coming from the external network.
Public telephone line/network	Line/network for sending/receiving fax data.
Fax data	Sent/received data in the public telephone line for faxes.
Certificate	Defined in ITU-T recommendation X.509. A certificate includes the data for user authentication (name, distinguished name, organization which the user belongs to, etc.), public key, expiry date, serial number, signature, etc.
Data on minimum user password length	Minimum user password length to set the user password on the MFD control panel. Included in the TOE setting data.
Key Operator password	Password data for Key Operator authentication. Included in the TOE setting data.
SA password	Password data for SA authentication. Included in the TOE setting data.
U.Normal password	Password data for general user (U.NORMAL) authentication. Included in the TOE setting data.
Data on access denial due to authentication failures	The data on whether to enable/disable access denial due to authentication failure. They also incorporate the data on the allowable number of the failures before access denial. Included in the TOE setting data.
Data on auditing	The data on whether to enable/disable the function to trace/record auditable events including important events of the TOE, such as device failure, configuration change, and user operation based on when and who operated what function. Included in the TOE setting data.
Data on user authentication	The data on whether to enable/disable the authentication function. The authentication function is performed using the user authentication information when copy, scan, fax, and print functions of MFD are performed. It also incorporates the data on the authentication method. Included in the TOE setting data.
Data on use of password entered from MFD control panel in user authentication	The data on whether to enable/disable the use of password when the user authentication is performed on the control panel. Included in the TOE setting data.
Data on Private Charge Print	The setting data on whether to store the received print data to Private Print area or print it out. Included in the TOE setting data.
Data on trusted communications	Data on whether the general encrypted communication protocols (TLS/HTTPS and TLS) are enabled/disabled and their detailed settings and certificate, authentication passwords, encryption keys, and shared keys to protect communication data in the internal network such as document data, job

	information, security audit log data, and TOE setting data. Included in the TOE setting data.
Data on Customer Engineer operation restriction	The data on whether to enable/disable the Customer Engineer Operation Restriction function and the data on the maintenance password. Included in the TOE setting data.
Data on Overwrite Storage	The data on whether to enable/disable the functions related to Overwrite Storage. Included in the TOE setting data.
Data on storage data encryption	The data on whether to enable/disable the functions related to storage data encryption. Included in the TOE setting data.
Data on date and time	The time zone / summer time information and the present time data. Included in the TOE setting data.
Data on Auto Clear	The data on whether to enable/disable the functions of Auto Clear and the timing to clear on the control panel and CWIS. Included in the TOE setting data.
Data on Self Test	The data on whether to enable/disable the Self Test function. Included in the TOE setting data.
Data on Report Print	The data on whether to enable/disable the Report Print function. Included in the TOE setting data.
Data on Firmware update	The setting data on firmware update functions. Setting data of Firmware Update. Included in the TOE setting data.

9. REFERENCES

[1] E. Barker , J. Kelsey, "SP 800-90A Rev.1 Recommendation for Random Number Generation UsingDeterministic Random Bit Generators," June 2015.

[2] National Institute of Standards and Technology, "FIPS 186-4 Digital Signature Standard (DSS)," July 2013.

[3] E. Barker, L. Chen, A. Roginsky, A. Vassilev , R. Davis, "SP 800-56A Rev. 3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography," April 2018.

[4] E. Barker, L. Chen, A. Roginsky, A. Vassilev, R. Davis , S. Simon, "SP 800-56B Rev. 2 Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography," March 2019.

[5] M. Dworkin, "SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques," December 2001.

[6] M. Dworkin, "SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," November 2007.

[7] National Institute of Standards and Technology, "FIPS 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES)," November 2001.

[8] "ISO/IEC 10118-3:2004," March 2004.

[9] "ISO/IEC 18033-3:2010," December 2010.

[10] "ISO/IEC 10116:2017," July 2017.

[11] National Institute of Standards and Technology, "FIPS 180-3 Secure Hash Standard (SHS)," March 2012.

[12] National Institute of Standards and Technology, "FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC)," July 2008.

[13] "RFC2818 HTTP Over TLS," May 2000.

[14] "RFC5246 The Transport Layer Security (TLS) Protocol Version 1.2," August 2008.