RICOH

imagine. change.

RICOH IM C401F/C401SRF/C431/C431F, version JE-1.00-H

Security Target

Version 1.3

August 2025

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
1.0	24 Jun 2025	Released to CB.
1.1	16 Jul 2025	Address OR
1.2	24 Jul 2025	Address OR
1.3	7 Aug 2025	Update secure boot claim.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the RICOH IM C401F/C401SRF/C431/C431F, version JE-1.00-H Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	RICOH IM C401F/C401SRF/C431/C431F, version JE-1.00-H
Security Target	RICOH IM C401F/C401SRF/C431/C431F, version JE-1.00-H Security Target, v1.3

2 **Note**: The TOE version (JE-1.00-H) is the collection of an alternative set of firmware packages. The complete list of firmware packages and versions can be found in Section 1.3.2 of the CC Guide.

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 revision 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) Collaborative Protection Profile for Hardcopy Devices, v1.0e

e) NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name	Applicability Rationale
TD0926	HIT Technical Decision: Clarification on FPT_SBT_EXT.1 Root of Trust	Applicable.
TD0927	HIT Technical Decision: Clarification on FPT_KYP_EXT.1 when using TPM-like device	Applicable.
TD0928	HIT Technical Decision: FCS_SSHC_EXT.1.8 and FCS_SSHS_EXT.1.8 Time based test case as optional	Not Applicable. TOE does not claim FCS_SSHC_EXT.1 or FCS_SSHS_EXT.1.

1.4 Terminology

Table 3: Terminology

Term	Definition
AES	Advanced Encryption Standard
BEV	Border Encryption Value
CBC	Cipher Block Chaining
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Service
CEM	Common Methodology for Information Security Evaluation
cPP	collaborative Protection Profile
DEK	Data Encryption Key
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
eMMC	embedded MultiMediaCard – A non-field-replaceable non-volatile memory storage device that the TOE uses to store documents and user account information.
FIPS	Federal Information Processing Standards
FTP Server	An external IT entity used by the TOE for file transfer.
GCM	Galois/Counter Mode
HCD	Hardcopy Device
HCDcPP	Collaborative Protection Profile for Hardcopy Devices, v1.0e
HMAC	keyed-hash message authentication code
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identification and Authentication
IPsec	Internet Protocol Security
IT	Information Technology

Term	Definition
iTC	international Technical Community
KDF	Key Derivation Function
KMD	Key Management Description
LAN	Local Area Network
LDAP Server	An external IT entity used by the TOE for network authentication of users.
MFD	Multifunction Device
MFP	Multifunction Printer, Multifunction Peripheral
NAT	Network address translation
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OSP	Organizational Security Policy
PP	Protection Profile
PSTN	Public Switched Telephone Network
PSTN Line	A connection to a public switched telephone network for the TOE to communicate with external fax machines
RBG	Random Bit Generator
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest–Shamir–Adleman
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMTP Server	An external IT entity used by the TOE for e-mail transmission

Term	Definition
Syslog Server	An external IT entity used by the TOE for audit log storage
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

2 TOE Description

2.1 Type

4 The TOE is a Digital Multi-Function Printer (MFP), which is an IT device that inputs, stores, and outputs electronic and hardcopy documents.

2.2 Usage

5 The expected use cases for the TOE are:

a) **Scanning.** The TOE scans paper documents and then transmits and deletes the scanned images, on command from the Operation Panel.

b) **Printing.** The TOE prints or stores documents received from a printer driver installed on the client computer and prints or deletes previously stored documents from the Operation Panel or the client computer's web browser.

c) **Copying.** The TOE scans paper documents to be printed.

d) **Network Communications**. The TOE is connected to its operational environment through a local area network (hereafter "LAN") and the public switched telephone network (PSTN). It sends and receives documents over the LAN and the PSTN.

e) **Administration.** The TOE provides management functions to configure and manage its operation. The management functions are accessible locally from the Operation Panel or remotely through the Web Image Monitor (hereafter "WIM") accessible using a web browser on a client computer.

f) **PSTN Faxing.** The TOE provides fax transmission and fax reception functions; both exchange documents according to the Group 3 standard over a Public Switch Telephone Network (PSTN). The Fax Transmission Function sends scanned images of paper documents, or images of electronic documents from a client computer, to external fax devices. The Fax Reception Function receives documents from external fax devices, and stores them in the TOE.

g) **Storage and Retrieval.** The TOE provides a Document Server Function which stores documents and allows users to perform operations on persistently stored documents. From the operation panel, users can store, print and delete documents stored by the document server. From a client computer, users can print and delete documents stored by the document server.

h) **Field-Replaceable Non-volatile Storage.** The TOE stores encrypted data both in the SSD and in NVRAM.

i) **Internal Audit Log Storage.** The MFP stores its audit data internally on the local device in addition to providing the capability for storing them externally to a remote syslog server.

2.2.1 Deployment

6 As shown in Figure 1, the TOE is connected to its operational environment through a local area network (hereafter "LAN") and the public switched telephone network (PSTN). Other elements of the TOE's operational environment are as shown.

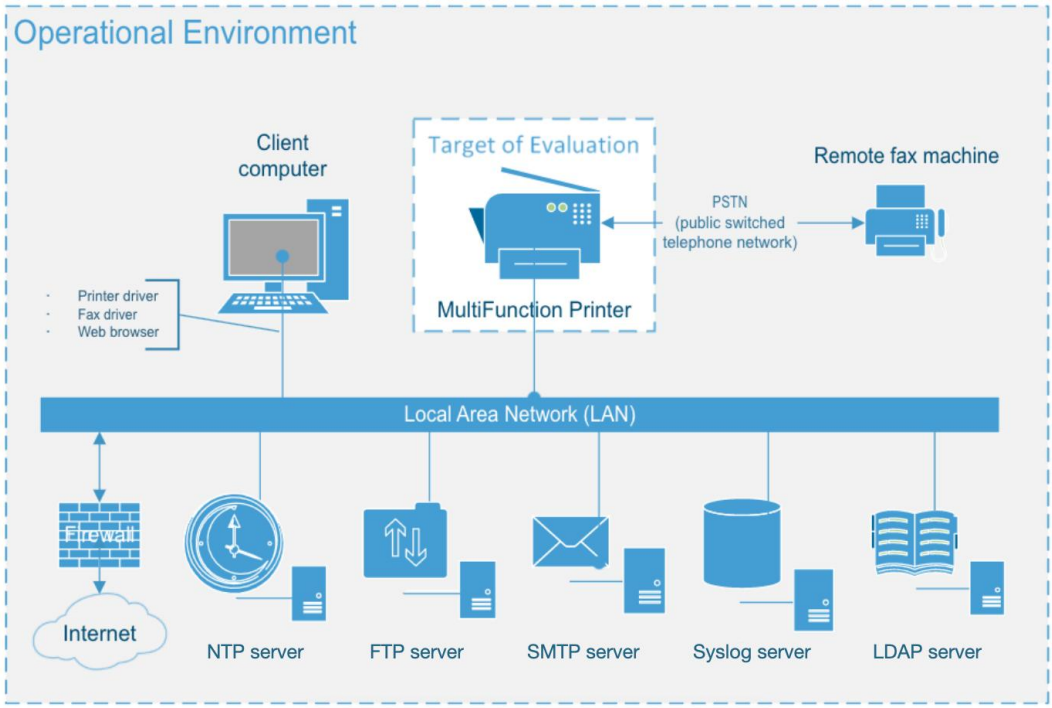

Figure 1: Example TOE deployment

2.2.2 Interfaces

7 The TOE interfaces include the following:

a) **Operation Panel of the MFP** is an LCD touch screen interface that provides a local user interface where users can perform the following operations:

   i. Configuration of the MFP

   ii. Copying, faxing, storage, and network transmission of paper documents

   iii. Printing, faxing, network transmission, and deletion of the stored documents

   iv. Receiving fax documents via telephone lines and storing them

b) **Web Image Monitor (WIM)** this is the remote user interface accessible via TLS/HTTPS where users can perform the following operations:

   i. Limited configuration of the MFP – various settings

   ii. Printing of documents

   iii. Faxing of documents

c) **Client printer driver or fax driver** is a remote user interface where communication is protected using TLS.

d) **IPsec interface** is used by the TOE to communicate with LDAP, syslog, NTP, SMTP and FTP servers in the TOE operational environment.

e) **PSTN Fax Line** is used to connect to a remote fax machine.

2.3 Physical Scope

8 The physical boundary of the TOE is comprised of the software and hardware of the MFP models identified in Table 4 (which shows the different RICOH Family Group brand names for the TOE) and related guidance documentation. The TOE is delivered by commercial courier and is installed with the assistance of a RICOH customer engineer.

9 The differences between models are not security relevant and are limited to branding variations (labels, displays, packaging materials and documentation).

10 The TOE is equipped with an SSD for non-volatile mass storage.

Table 4: TOE Models

Branding	Model
RICOH	IM C401F, IM C401SRF, RICOH IM C431, RICOH IM C431F
nashuatec	IM C401F, IM C401SRF
Rex Rotary	
Gestetner	

Note: Models sold in Japan include RICOH in the model's name.

11 The TOE includes the following critical components:

a) **Controller.** Provides primary printing, scanning, faxing, and networking functionality.

   i) **CPU.** Intel Atom x5-E3930.

   ii) **OS.** Linux 4.14 (customized).

b) **Smart Operation Panel (SOP).** Provides front panel interface control and device extensibility capabilities.

   i) **CPU.** ARM Cortex-A57 Dual Core.

   ii) **OS.** Linux 4.19 (customized).

c) **TPM.** Used for key storage and entropy generation.

   i) STMicroelectronics ST33HTPH2X32AHE4, v1.769.

2.3.1 Guidance Documents

12 The TOE guidance documentation shown below is available through the vendor's support portal. The Common Criteria Guide is provided by the vendor upon request.

a) RICOH IM C401F/C401SRF/C431/C431F, version JE-1.00-H Common Criteria Guide, v1.0 (PDF)

b) User Guide IM C401F/C401SRF, D0FQ7073-EN 2024/11 (HTML)

c) Security Reference, D0FQ7074-EN 2024/11 (HTML)

2.4 Logical Scope

13 The logical scope of the TOE comprises the security functions provided by the TOE to include:

a) **Security Audit.** The TOE generates audit records of user and administrator actions. It stores audit records both locally and on a remote syslog server.

b) **Cryptographic Support.** The TOE includes multiple cryptographic modules for the cryptographic operations that it performs. The relevant CAVP certificate numbers are noted in Table 5 below.

c) **Access Control.** The TOE enforces access control policy to restrict access to user data. The TOE ensures that documents, document processing job information, and security-relevant data are accessible only to authenticated users who have the appropriate access permissions.

d) **Storage Data Encryption.** The TOE encrypts data on the SSD and in NVRAM to protect documents and confidential system information if those devices are removed from the TOE.

e) **Identification and Authentication.** Except for a defined minimal set of actions that can be performed by an unauthenticated user, the TOE ensures that all users must be authenticated before accessing its functions and data. Users log in to the TOE by entering their credentials on the local operation panel, through WIM login, through print or fax drivers, or using network authentication services.

f) **Administrative Roles.** The TOE provides the capability for managing its functions and data. Role-based access controls ensure that the ability to configure the security settings of the TOE is available only to the authorized administrators. Authenticated users can perform copy, printer, scanner and fax operations based on the user role and the assigned permissions.

g) **Trusted Operations.** The TOE performs power-on self-tests to ensure the integrity of the TSF components. It provides a mechanism for performing trusted update that verifies the integrity and authenticity of the upgrade software before applying the updates.

h) **TOE Access.** Interactive user sessions at the local and remote user interfaces are automatically terminated by the TOE after a configured period of inactivity.

i) **Trusted Communications.** The TOE protects communications from its remote users using TLS/HTTPS, and communications with the syslog, SMTP LDAP, FTP and NTP servers using IPsec.

j) **PSTN Fax-Network Separation.** The TOE restricts information received from or transmitted to the telephone network to only fax data and fax protocols. It ensures that the fax modem cannot be used to bridge the LAN.

2.4.1 CAVP Certificates

14 The TOE includes the cryptographic modules with related CAVP certificates shown Table 5 below.

Table 5: CAVP Certificates

Module	Operating Environment	Algorithms	CAVP	Usage
OpenSSL, v1.1.1	Linux 4.14 on Intel Atom Apollo Lake E3930 (Goldmont)	AES-CBC SHA-256 SHA-384 SHA-512 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 RSA Signature Verification (2048-bit, SHA-256, PKCS#1 v1.5) FIPS 186-4 KAS-FFC CTR DRBG RSA Signature Generation (2048-bit, SHA-256, SHA-384, SHA-512, PKCS#1 v1.5) FIPS 186-4	A3561	TLS
Ricoh Cryptographic Module for IPsec 2, v1.00	Linux 4.14 on Intel Atom Apollo Lake E3930 (Goldmont)	AES-CBC SHA-256 SHA-384 SHA-512 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	A3560	IPsec P2
RICOH Platform Validation Library for JX3, v1.0	BIOS on Intel Atom Apollo Lake E3930 (Goldmont)	SHA-256	A6516	Self-test (integrity)
Libgwguard, v1.0	Linux 4.14 on Intel Atom Apollo Lake E3930 (Goldmont)	SHA-256 RSA Signature Verification (2048-bit, SHA-256, PKCS#1 v1.5) FIPS 186-4	A3558	signature verification (firmware update)
RICOH Cryptographic	Linux 4.14 on Intel Atom Apollo	SHA-256 RSA Signature Verification (2048-bit,	A3559	Self-test (integrity) - MFP

Module	Operating Environment	Algorithms	CAVP	Usage
Library for ima, v1.0	Lake E3930 (Goldmont)	SHA-256, PKCS#1 v1.5) FIPS 186-4		
Libimaevm, v1.0	Linux 4.14 on Intel Atom Apollo Lake E3930 (Goldmont)	SHA-256 RSA Signature Generation (2048-bit, SHA-256, PKCS#1 v1.5) FIPS 186-4	A3562	firmware integrity of verification (startup)
GW Linux NVRAM Encryption Library, v1.0	Linux 4.14 on Intel Atom Apollo Lake E3930 (Goldmont)	AES-CBC	A3555	MFP controller
AES256CBC, v MB8AL1062MH-GE1	AES256CBC	AES-CBC Encryption/decryption key length 256	AES 3921	AES 256bit-CBC
RICOH RSA Module for U-boot, v1.1.0	Customized U-Boot 2018.09 on ARM Cortex-A57	RSA Signature Verification (4096-bit, SHA-256, PKCS#1 v1.5) FIPS 186-4	A5472	Self-test (integrity) - SOP
RICOH SHA256 Module for U-boot, v1.1.0	Customized U-Boot 2018.09 on ARM Cortex-A57	SHA-256	A5473	Self-test (integrity) - SOP
RICOH Cryptographic Library for Linux Kernel, v1.0.0	Customized Linux 4.19 on ARM Cortex-A57	SHA-256	A5471	Self-test (integrity) - SOP
RICOH Cryptographic Library 3, v3.0	Customized Linux 4.19 on ARM Cortex-A57	SHA-256 RSA Signature Verification (2048-bit, SHA-256, PKCS#1 v1.5) FIPS 186-4	A3557	Trusted Update – SOP Software (Apps)
NesLib, v6.5 for ST33	SecureCore® SC300	SHA-256 Hash_DRBG (SHA-256)	A1288	Entropy source for other DRBGs Secure Boot
wolfCrypt, v4.7.0i	Linux 4.14 on Intel Atom Apollo Lake E3930 (Goldmont)	RSA Key Generation RSA Signature Generation (2048-bit, SHA-256, SHA-384, SHA-512, PKCS#1 v1.5) FIPS 186-4	A3028	TLS/HTTPS

Module	Operating Environment	Algorithms	CAVP	Usage
		RSA Signature Generation (4096-bit, SHA-256, SHA-384, SHA-512, PKCS#1 v1.5) FIPS 186-4 RSA Signature Verification (2048-bit, SHA-256, SHA-384, SHA-512, PKCS#1 v1.5) FIPS 186-4 RSA Signature Verification (4096-bit, SHA-256, SHA-384, SHA-512, PKCS#1 v1.5) FIPS 186-4		
		ECDSA Key Generation Curve (P-256, P-384, P-521) ECDSA Key Verification Curve (P-256, P-384, P-521)		
		SHA-256, SHA-384, SHA-512		
		AES-CBC AES-GCM Encryption/decryption Key length 128, 256		
		HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512		
		Hash DRBG		
		KAS-ECC-SSC		
		KAS-FFC-SSC		

2.4.2 Excluded Features

15 The following features of the MFP are excluded from the evaluated configuration:

a) **USB Port.** The MFP has a USB Port that is used to directly connect a client computer to the MFP for printing. This USB port is disabled during initial installation and configuration of the TOE.

b) **SD Card Slot.** The MFP has two SD Card Slots, one for customer engineers and one for users. The SD Card Slot for customer engineer is used by customer engineers to install components of the MFP; the SD Card Slot for users is used by users to print documents. Both are disabled when the TOE is operational, a cover is placed on the SD Card slot for customer engineer so cards cannot be inserted or removed and the card slot for users is set to disabled during installation.

2.4.3 Required non-TOE Components

16 The following non-TOE components are required in the TOE operational environment:

a) **Syslog Server.** The TOE uses a remote syslog server for long term storage of its audit trail.

b) **LDAP Server.** The TOE uses an LDAP server for user authentication.

c) **NTP Server.** The TOE ensures accurate time by synchronizing with a remote NTP server.

d) **FTP Server.** The TOE stores user documents on a remote FTP server.

e) **SMTP Server.** The TOE uses an SMTP server for email transmission.

3 Security Problem Definition

17 The Security Problem Definition is reproduced from Section 3 and Appendix I of the HCDcPP.

3.1 Users

18 There are two categories of Users defined in this ST, Normal and Admin.

Table 6: User Categories

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

19 A conforming TOE may allow additional roles, sub-roles, or groups. In particular, a conforming TOE may allow several administrative roles that have authority to administer different aspects of the TOE.

3.2 Assets

20 Assets are passive entities in the TOE that contain or receive information. In this HCDcPP, Assets are Objects (as defined by the CC). There are two categories of Assets defined in this HCDcPP:

Table 7: Asset Categories

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

21 There are no additional Asset categories defined in this ST.

3.2.1 User Data

22 User Data are composed of two types:

Table 8: User Data Types

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.

23 There are no additional types of User Data defined in this ST. Attributes associate documents and document processing jobs with the document processing functions of the TOE:

Table 9: Document and Job Attributes

Document processing function	Attribute
Printing	+PRT
Copying	+CPY
Scanning	+SCN
Fax (reception)	+FAXIN
Fax (transmission)	+FAXOUT
Document Storage/Retrieval	+DSR

3.2.2 TSF Data

24 TSF Data are composed of two types:

Table 10: TSF Data Types

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.

25 There are no additional TSF Data types defined in this ST.

3.3 Threats

26 The following threats are mitigated by this TOE:

Table 11: Threats

Identifier	Description
T.UNAUTHORIZED_ ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.

Identifier	Description
T.TSF_FAILURE	A malfunction of the TSF may compromise the device security status if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may install unauthorized firmware/software on the TOE to modify the Device security status.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.
T.WEAK_CRYPTO	An attacker may exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes to access (read, modify, or delete) TSF and User data.

3.4 Assumptions

27 The following assumptions must be satisfied in order for the Security Objectives and Security Functional Requirements to be effective:

Table 12: Assumptions

Identifier	Description
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.

3.5 Organizational Security Policies

28 The following Organizational Security Policies (OSPs) are enforced by this TOE:

Table 13: Organizational Security Policies

Identifier	Description
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 stored within the TOE as well as protected and transmitted to an External IT Entity.

Identifier	Description
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for 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.ROT_INTEGRITY	The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters.

4 Security Objectives

29 The following Security Objectives are satisfied by this TOE:

Table 14: Security Objectives for the TOE

Identifier	Description
O.USER_I&A	The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles.
O.ACCESS_CONTROL	The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
O.USER_AUTHORIZATION	The TOE shall perform authorization of Users in accordance with security policies.
O.ADMIN_ROLES	The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.
O.UPDATE_VERIFICATION	The TOE shall provide mechanisms to verify the authenticity of firmware/software updates.
O.TSF_SELF_TEST	The TOE shall test some subset of its security functionality to help ensure that subset is operating properly.
O.COMMS_PROTECTION	The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.

Identifier	Description
O.AUDIT	The TOE shall generate audit data and store it internally as well as be capable of sending it to a trusted External IT Entity.
O.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data in Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices.
O.KEY_MATERIAL	The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material.
O.FAX_NET_SEPARATION(conditionally mandatory)	If the TOE provides a PSTN fax function, then the TOE shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function.
O.AUTH_FAILURES (conditi onally mandatory)	The TOE resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.
O.FW_INTEGRITY	The TOE ensures its own integrity has remained intact and attests its integrity to outside parties on request.
O.STRONG_CRYPTO	The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards, including support for random bit generation based on recognized standards and a source of sufficient entropy. The TOE uses key sizes that are recognized as providing sufficient resistance to current attack capabilities.

30 The following Security Objectives must be satisfied by the TOE's Operational Environment.

Table 15: Security Objectives for the Operational Environment

Identifier	Description
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.

Identifier	Description
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 Security Requirements

5.1 Conventions

31 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment**. Indicated with italicized text.

b) **Refinement**. Indicated with bold text and strikethroughs.

c) **Selection**. Indicated with underlined text.

d) **Assignment within a Selection**: Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding letter in parentheses for iterations completed in the PP. Iterations completed in the ST are identified by adding a string starting "/" (e.g. "FCS_CKM.1/SKG").

Note: operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the HCDcPP.

5.2 Extended Components Definition

32 The following list identifies the extended components used in this ST. All extended components are drawn from the HCDcPP.

- FAU_STG_EXT.1
- FCS_CKM_EXT.4
- FCS_IPSEC_EXT.1
- FCS_HTTPS_EXT.1
- FCS_RBG_EXT.1
- FCS_TLSS_EXT.1
- FCS_KYC_EXT.1
- FDP_FXS_EXT.1
- FDP_DSK_EXT.1
- FIA_PMG_EXT.1
- FPT_SBT_EXT.1
- FPT_SKP_EXT.1
- FPT_TST_EXT.1
- FPT_TUD_EXT.1
- FPT_KYP_EXT.1
- FIA_PSK_EXT.1
- FIA_X509_EXT.1
- FIA_X509_EXT.2
- FIA_X509_EXT.3

5.3 Functional Requirements

Table 16: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_STG.1	Protected Audit Trail Storage
FAU_STG_EXT.1	Extended: External Audit Trail Storage
FAU_STG.4	Prevention of Audit Data Loss
FCS_CKM.1/AKG	Cryptographic Key Generation (Asymmetric keys)
FCS_CKM.1/SKG	Cryptographic Key Generation (Symmetric keys)
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM_EXT.4	Extended: Cryptographic Key Material Destruction
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (Symmetric Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_COP.1/KeyEnc	Cryptographic operation (Key Encryption)
FCS_COP.1/StorageEncryption	Cryptographic Operation (Data Encryption/Decryption)
FCS_HTTPS_EXT.1	Extended: HTTPS selected
FCS_IPSEC_EXT.1	Extended: IPsec selected
FCS_RBG_EXT.1	Extended: Random Bit Generation
FCS_TLSS_EXT.1	TLS Server Protocol Without Mutual Authentication
FCS_KYC_EXT.1	Extended: Key Chaining

Requirement	Title
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security attribute based access control
FDP_FXS_EXT.1	Extended: Fax separation
FDP_DSK_EXT.1	Extended: Protection of Data on Disk
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User attribute definition
FIA_PMG_EXT.1	Extended: Password Management
FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FIA_X509_EXT.1	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_SBT_EXT.1	Extended: Secure Boot
FPT_SKP_EXT.1	Extended: Protection of TSF Data
FPT_STM.1	Reliable Time Stamps
FPT_TST_EXT.1	Extended: TSF testing

Requirement	Title
FPT_TUD_EXT.1	Extended: Trusted update
FPT_KYP_EXT.1	Extended: Protection of Key and Key Material
FTA_SSL.3	TSF-initiated Termination
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1/Admin	Trusted Path (for Administrators)
FTP_TRP.1/NonAdmin	Trusted Path (for Non-administrators)

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

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 17, [*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 17**, [*no other audit relevant information*].

Table 17: Audit Events

Auditable Event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful login attempts limit is met or exceeded	FIA_AFL.1	None
Unsuccessful User authentication	FIA_UAU.1	Supplied User ID/Name and origin of the attempt (e.g., IP address)
Unsuccessful User identification	FIA_UID.1	Supplied User ID/Name and origin of the attempt (e.g., IP address)

Auditable Event	Relevant SFR	Additional information
Unsuccessful attempt to validate a certificate	FIA_X509_EXT.1	Reason for failure of certificate validation
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/Admin, FTP_TRP.1/NonAdmin	Reason for failure

FAU_GEN.2 User Identity Association

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

FAU_SAR.1.1 The TSF shall provide **[an Administrator]** 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

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

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_EXT.1 Extended: External Audit Trail Storage

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.

FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 Refinement The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

5.3.2 Cryptographic Support (FCS)

FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric keys)

FCS_CKM.1.1/AKG Refinement: The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using ‘NIST curves’ [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
- FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526, RFC 7919].

].

FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric keys)

FCS_CKM.1.1/SKG Refinement: The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1** and specified cryptographic key sizes [128 bits, 256 bits] that meet the following: [NIST SP 800-133 Rev.2 Section [6.1]].

FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1 **Refinement** The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”
- FFC Schemes using “safe-prime” groups that meet the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526, RFC 7919].

].

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

FCS_CKM.4 Cryptographic Key Destruction

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

- For volatile memory, the destruction shall be executed by a [removal of power to the memory];
- For non-volatile storage that consists of the invocation of an interface provided by the underlying platform that [
    - logically addresses the storage location of the key and performs a [single] overwrite consisting of [a new value of a key of the same size]];
    - instructs the underlying platform to destroy the abstraction that represents the key

] that meets the following: [*No Standard]*.

FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption The TSF shall perform **[encryption/decryption]** in accordance with specified cryptographic algorithms [

- AES used in [CBC, GCM] mode

] and cryptographic key sizes [

Case: AES algorithm

- [128 bits, 192 bits, 256 bits]

] that meet the following [

Case: AES algorithm

- ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772]

].

FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption)

FCS_COP.1.1/KeyEnc Refinement: The TSF shall perform [**key encryption and decryption**] in accordance with a specified cryptographic algorithm [

Case: AES algorithm

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

].

FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen The TSF shall perform [**cryptographic signature services (generation and verification)**] in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits,4096 bits*]]

that meets the following: [

Case: RSA schemes:

- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

].

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash Refinement: The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [**SHA-256, SHA-384, SHA-512**] and message digest sizes [**256, 384, 512] bits** that meet the following: [**ISO/IEC 10118-3:2004**].

FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash Refinement: The TSF shall perform [**keyed-hash message authentication**] in accordance with a specified cryptographic algorithm [HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [*512*,*1024*] **and message digest sizes [256, 384, 512] bits** that meet the following: [**ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”**].

FCS_HTTPS_EXT.1 Extended: HTTPS 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_TLSS_EXT.1 and/or FCS_TLSC_EXT.1.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [not require client authentication, [*no other action*]] if the peer certificate is deemed invalid.

FCS_IPSEC_EXT.1 Extended: IPsec selected

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

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [transport mode, tunnel mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [AES-CBC-128 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC 3602)] together with a

Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers], and [RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1] protocol uses the cryptographic algorithms [AES-CBC-128, AES-CBC-192, AES-CBC-256 (specified in RFC 3602)].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on [length of time, where the values can be configured within [*1-24*] hours;];

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on [length of time, where the values can be configured within [*1-8*] hours;];

].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in gx mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*224*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv1] exchanges of length [

- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [

- [14 (2048-bit MODP)] according to RFC 3526

].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 1] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [RSA] that use X.509v3 certificates that conform to RFC 4945 and [Pre-shared Keys].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [Distinguished Name (DN)] and [no other reference identifier type].

FCS_RBG_EXT.1 Extended: Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [Hash_DRBG (**~~any~~ SHA-256**), CTR_DRBG(**~~AES~~ AES-256**)].

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

FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 3268

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 3268

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [TLS 1.1].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves]].

FCS_TLSS_EXT.1.4 The TSF shall support [session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2)].

FCS_KYC_EXT.1 Extended: Key Chaining

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

FCS_COP.1/StorageEncryption Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1/StorageEncryption The TSF shall perform [**data encryption and decryption**] in accordance with specified cryptographic algorithms [

- AES used in [CBC] mode

] and cryptographic key sizes [

Case: AES algorithm

- [256 bits]

] that meet the following [

Case: AES algorithm

- ISO 18033-3, [CBC as specified in ISO 10116]

].

5.3.3 User Data Protection (FDP)

FDP_ACC.1 Subset 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 4 and Table5**~~ Table 18 **and** Table 19**.**

FDP_ACF.1 Security attribute based access control

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 4 and Table5**~~ Table 18 **and** Table 19**.**

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 4 and Table5~~** Table 18 **and** Table 19**.**

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

Table 18: D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print (+PRT)	Operation:	Submit a document to be printed	View image or Release printed output	Modify stored document	Delete stored document
	Job owner	Allowed (note 1)	View: Allowed Release: Allowed	Denied	Allowed
	U.ADMIN	Denied	View: Denied Release: Denied	Denied	Allowed
	U.NORMAL	Allowed	Denied	Denied	Denied
	Unauthenticated	(condition 1)	Denied	Denied	Denied
Scan (+SCN)	Operation:	Submit a document for scanning	View scanned image	Modify stored image	Delete stored image
	Job owner	Allowed (note 2)	Allowed	Denied	Allowed
	U.ADMIN	Denied	Denied	Denied	Allowed
	U.NORMAL	Allowed	Denied	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Copy (+CPY)	Operation:	Submit a document for copying	View scanned image or Release printed copy output	Modify stored image	Delete stored image
	Job owner	Allowed (note 2)	View: Denied Release: Denied	Denied	Denied

		"Create"	"Read"	"Modify"	"Delete"
	U.ADMIN	Denied	View: Denied Release: Denied	Denied	Denied
	U.NORMAL	Allowed	Denied	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Fax send (+FAXOUT)	Operation:	Submit a document to send as a fax	View scanned image	Modify stored image	Delete stored image
	Job owner	Allowed (note 2)	Allowed	Denied	Allowed
	U.ADMIN	Denied	Denied	Denied	Allowed
	U.NORMAL	Allowed	Denied	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Fax receive (+FAXIN)	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	Allowed (note 3)	View: Allowed Release: Allowed	Denied	Allowed
	U.ADMIN	Allowed (note 4)	View: Denied Release: Denied	Denied	Denied
	U.NORMAL	Allowed (note 4)	Denied	Denied	Denied
	Unauthenticated	Allowed	Denied	Denied	Denied
Storage/ Retrieval (+DSR)	Operation:	Store document	Retrieve stored document	Modify stored document	Delete stored document
	Job owner	Allowed	Allowed	Denied	Allowed

		"Create"	"Read"	"Modify"	"Delete"
		(note 1)			
	U.ADMIN	Denied	Denied	Denied	Allowed
	U.NORMAL	Allowed	Denied	Denied	Denied
	Unauthenticated	(condition 1)	Denied	Denied	Denied

Table 19: D.USER.JOB Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print (+PRT)	Operation:	Create print job	View print queue / job	Modify print job	Cancel print job
	Job owner	(note 1)	Allowed	Denied	Allowed
	U.ADMIN	Denied	Allowed	Denied	Allowed
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	(condition 1)	Allowed	Denied	Denied
Scan (+SCN)	Operation:	Create scan job	View scan status / log	Modify scan job	Cancel scan job
	Job owner	(note 2)	Allowed	Denied	Allowed
	U.ADMIN	Denied	Allowed	Denied	Allowed
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Copy (+CPY)	Operation:	Create copy job	View copy status / log	Modify copy job	Cancel copy job
	Job owner	(note 2)	Allowed	Denied	Allowed
	U.ADMIN	Denied	Allowed	Denied	Denied
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Fax send (+FAXOUT)	Operation:	Create fax send job	View fax job queue / log	Modify fax send job	Cancel fax send job

		"Create"	"Read"	"Modify"	"Delete"
	Job owner	(note 2)	Allowed	Allowed	Denied
	U.ADMIN	Denied	Allowed	Denied	Denied
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Fax receive (+FAXIN)	Operation:	Create fax receive job	View fax receive status / log	Modify fax receive job	Cancel fax receive job
	Fax owner	(note 3)	Allowed	Denied	Allowed
	U.ADMIN	(note 4)	Allowed	Denied	Allowed
	U.NORMAL	(note 4)	Allowed	Denied	Denied
	Unauthenticated	Allowed	Denied	Denied	Denied
Storage/ Retrieval (+DSR)	Operation:	Create storage / retrieval job	View storage / retrieval log	Modify storage / retrieval job	Cancel storage / retrieval job
	Job owner	(note 1)	Allowed	Denied	Denied
	U.ADMIN	Denied	Allowed	Denied	Denied
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	(condition 1)	Denied	Denied	Denied

Application notes:

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

See also the following Notes that are referenced in ~~**Table 4 and Table5**~~ Table 18 **and** Table 19**.**

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

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

Note 3: Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of received faxes is assigned to a specific user or U.ADMIN role.

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

FDP_FXS_EXT.1 Extended: Fax separation

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

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

FDP_DSK_EXT.1.1 The TSF shall [perform encryption in accordance with FCS_COP.1/ StorageEncryption], such that any 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.

5.3.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*1 to 10*]] unsuccessful authentication attempts occur related to [

- *User authentication using the Operation Panel*
- *User authentication using WIM from the client computer*
- *User authentication when printing from the client computer*
- *User authentication when using LAN Fax from the client computer*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the user account for an administrator configurable time period, or until an administrator unlocks the account*.].

Application Note: This SFR applies only to internal identification and authentication.

FIA_ATD.1 User attribute definition

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

FIA_PMG_EXT.1 Extended: Password Management

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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, *[[“”“, “”“, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[“, “\”, “]”, “_”, “`”, “{“, “|”, “}”, “~”]]*;
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [*1-32 characters*];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [SHA-256, SHA-384, SHA-512] and be able to [use no other pre-shared keys].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 Refinement: The TSF shall allow [*the viewing of the list of user jobs, WIM Help, system status, counter and information of inquiries, creation of fax reception jobs, and creation of print or storage jobs*] 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

FIA_UAU.7.1 The TSF shall provide only [*displaying dummy characters as authentication feedback on the Operation Panel and through WIM*] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

FIA_UID.1.1 Refinement The TSF shall allow [*the viewing of the list of user jobs, WIM Help, system status, counter and information of inquiries, creation of fax reception jobs, and creation of print or storage jobs*] 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

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*username, available function list, and 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: [*an Available functions list is associated with the user after the user is authenticated*, *and the set of available functions does not change during the user session*.]

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

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev Refinement The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [IPsec] and [no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.3.5 Security Management (FMT)

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 Refinement The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*listed in Table 20*] to **U.ADMIN**.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 Refinement The TSF shall enforce **the User Data Access Control SFP** to restrict the ability to [query, modify] the security attributes [*username, available function list, user role]* to [*U.ADMIN*].

FMT_MSA.3 Static attribute initialization

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

FMT_MSA.3.2 Refinement The TSF shall allow the **[U.ADMIN]** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

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 ~~Table6~~** Table 20

Table 20: Management of TSF Data

Data	Operation	Interfaces	Authorized Role(s)
TSF Data owned by U.NORMAL or associated with documents or jobs owned by U.NORMAL.			
Login password for authenticated user	Modify	Operation Panel, WIM	The Owning U.NORMAL or U.ADMIN
TSF Data not owned by a U.NORMAL			
Audit Logs	Delete, export, query	WIM	U.ADMIN

Data	Operation	Interfaces	Authorized Role(s)
Login passwords of U.ADMIN user	Modify	Operation Panel, WIM	U.ADMIN
Username, available function list or access permissions of U.NORMAL Users	Modify	Operation Panel, WIM	U.ADMIN
Storage Key	Create, Delete	Operation Panel	U.ADMIN
Software, firmware, and related configuration data			
Audit Transfer Settings	Modify	Operation Panel, WIM	U.ADMIN
Date & Time Settings	Modify	WIM	U.ADMIN
Password Length and Password complexity settings	Modify	Operation Panel, WIM	U.ADMIN
Operation Panel Auto logout settings	Modify	Operation Panel, WIM	U.ADMIN
WIM Auto logout settings	Modify	WIM	U.ADMIN
Fax owner	Modify	Operation Panel, WIM	U.ADMIN
Device Certificate	Create, Modify, Delete, Upload	Operation Panel, WIM	U.ADMIN
CA Certificate	Import, Delete	WIM	U.ADMIN
TOE Software updates	Modify	WIM	U.ADMIN
Network settings for trusted communication	Modify	Operation Panel, WIM	U.ADMIN
SMTP over IPsec settings	Modify	WIM	U.ADMIN
Syslog over IPsec	Modify	WIM	U.ADMIN
NTP settings	Modify	WIM	U.ADMIN
TLS settings	Modify	WIM	U.ADMIN
IPsec settings	Modify	WIM	U.ADMIN

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*management functions listed in* Table 21].

Table 21: Management Functions

Management Functions	Operation	Interface(s)
Manage user accounts (users, roles, privileges and available functions list)	Create, Modify, Delete	Operation Panel, WIM
Configure audit transfer settings	Modify	WIM
Manage audit logs	Delete, Export, Query	Operation Panel, WIM
Manage Audit Functions	Enable, Disable	Operation Panel, WIM
Manage time and date settings	Modify	Operation Panel, WIM
Configure minimum password length	Modify	Operation Panel, WIM
Configure Password complexity settings	Modify	Operation Panel, WIM
Configure Operation Panel Auto Logout Time	Modify	Operation Panel
Configure WIM Auto Logout Time	Modify	WIM
Configure number of authentication failures before account lockout	Modify	Operation Panel, WIM
Configure account lockout timer settings	Modify	Operation Panel, WIM
Configure Fax owner	Modify	Operation Panel, WIM
Configure network settings for trusted communications (specify IP addresses and port to connect to the TOE)	Modify	Operation Panel, WIM
Manage Storage Key	Create, Modify, Delete	Operation Panel
Manage Device Certificates	Create, Modify, Delete, Upload	Operation Panel, WIM

Management Functions	Operation	Interface(s)
Manage CA Certificates	Import, Delete	WIM
Manage TOE Trusted Update	Query, Modify	WIM
Configure SMTP over IPsec	Modify	WIM
Configure syslog over IPsec	Modify	WIM
Configure NTP	Modify	WIM
Configure TLS	Modify	WIM
Manage user accounts (Ability to login)	Unlock	WIM

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [**U.ADMIN, U.NORMAL**].

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

5.3.6 Protection of the TSF (FPT)

FPT_SBT_EXT.1 Extended: Secure Boot

FPT_SBT_EXT.1.1 The TSF shall contain one or more chains of trust with each chain of trust anchored in an immutable Root of Trust.

FPT_SBT_EXT.1.2 At boot time the TSF shall use the chain(s) of trust to confirm integrity of its firmware/software using a [hash, digital signature] verification method.

FPT_SBT_EXT.1.3 The TSF shall [halt boot process [*a Service Call (SC) error code is displayed on the Operator Panel and the TOE becomes unavailable*]] in the event of a boot time verification failure so that the corrupted firmware/software isn't executed.

FPT_SBT_EXT.1.4 Following failure of verification, the TSF shall provide a mechanism to: [indicate a need to contact vendor support].

FPT_SBT_EXT.1.5 The TSF shall contain [hash data, public key for digital signature] in the Hardware Root of Trust.

FPT_SBT_EXT.1.6 The TSF shall make the symmetric key accessible only to the Hardware Root of Trust.

Application Note: This SFR has been modified by TD0926.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

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

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

FPT_TST_EXT.1 Extended: TSF testing

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

FPT_TUD_EXT.1 Extended: Trusted update

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 [digital signature] and [no other functions] prior to installing those updates.

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

FPT_KYP_EXT.1.1 The TSF shall [

- only store plaintext keys that meet any one of the following criteria [
    - The non-volatile memory where the key is stored on is located in a protected storage device]

    ].

Application Note: This SFR has been modified by TD0927.

5.3.7 TOE Access (FTA)

FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*settable from 10 to 999 seconds for operation panel and 3 to 60 minutes for WIM*].

5.3.8 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall **use [IPsec] to** provide **a trusted** communication channel between itself and **authorized IT entities**

supporting the following capabilities: remote audit server, [*authentication server, [File server, Network time server and Email 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 **remote audit** [***remote authentication, file transfer, network time synchronization and sending email***].

FTP_TRP.1/Admin Trusted Path (for Administrators)

FTP_TRP.1.1/Admin Refinement: The TSF shall **use [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/Admin Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3/Admin Refinement: The TSF shall require the use of the trusted path for [**initial administrator authentication and all remote administration actions**].

FTP_TRP.1/NonAdmin Trusted Path (for Non-administrators)

FTP_TRP.1.1/NonAdmin Refinement: The TSF shall **use [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/NonAdmin Refinement: The TSF shall permit [the TSF, remote users] to initiate communication via the trusted path.

FTP_TRP.1.3/NonAdmin Refinement: The TSF shall require the use of the trusted path for [**initial user authentication and all remote user actions**].

5.4 Assurance Requirements

33 The TOE security assurance requirements are summarized in Table 22. See Annex B for Security Assurance Requirements description.

Table 22: TOE Security Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation (ASE)	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)	ADV_FSP.1	Basic Functional Specification
Guidance Documents (AGD)	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support (ALC)	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests (ATE)	ATE_IND.1	Independent Testing - conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability survey

6 TOE Summary Specification

34 The following describes how the TOE fulfils each SFR included in section 5.3.

6.1 Security Audit

6.1.1 FAU_GEN.1 & FAU_GEN.2

35 The TOE records an audit log of events listed in Table 23. Audit log entries record the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Additionally, Job Completion events record the type of job, and Failure to Establish Session events record the reason for such failure.

Table 23: List of Audit Events

Auditable event requirements	Auditable events satisfied
Start-up and shutdown of the audit functions	Start-up of the Audit Function
	Shutdown of the Audit Function
Job completion	Printing via networks
	LAN Fax via networks
	Scanning documents
	Copying documents
	Receiving incoming faxes
	Reading document data (print, fax transmission)
	Deleting document data
Unsuccessful User authentication, Unsuccessful User identification	Failure of login operations
Use of management functions	Use of functions identified in FMT_SMF.1
Modification to the group of Users that are part of a role	Modification of MFP Administrator roles
Changes to the time	Date settings (year/month/day), time settings (hour/minute)
Failure to establish session	Failure of communication with the audit server
	Failure of communication with the authentication server

Auditable event requirements	Auditable events satisfied
	Failure of communication with the FTP server
	Failure of communication with the NTP server
	Failure of communication with print driver
	Failure of communication with fax driver
	Failure of communication with WIM
	Failure of communication with Email Server
Unsuccessful attempt to validate a certificate	Unsuccessful attempt to validate a certificate
	Reason for failure of certificate validation

6.1.2 FAU_STG.1, FAU_STG_EXT.1, FAU_STG.4, FAU_SAR.1, FAU_SAR.2 and FTP_ITC.1

36 The TOE stores audit log data in a dedicated storage area of the SSD. Audit records are buffered in that storage area before transfer to a configured remote syslog server over a configured IPsec trusted channel.

37 Authorized administrators use the WIM to review the audit trail and to initiate transfer of audit records. The TOE prevents unauthorized access to the audit records by ensuring that the options to manage the audit function and the audit records are not included in the lists of available functions visible to the U.NORMAL users.

38 The TOE audit trail comprises three types of audit logs: Job logs, Access logs, and Ecology logs. By default, the job and ecology logs will each hold a maximum of 4,000 records; the access log can have a maximum of 12,000 records. When a maximum number of records is reached, the records are overwritten based on the following criteria:

a) When syslog audit transfers are working, the oldest records which have been transferred to the syslog server are overwritten first.

b) If none of the logs have been transferred to the audit server, the oldest records are overwritten first.

6.2 Identification and Authentication

6.2.1 FIA_UAU.1, FIA_UID.1, FIA_UAU.7, FIA_ATD.1 & FIA_USB.1

39 For each individual user, the TOE maintains the user attributes: username, password, user role and available functions list regardless of the authentication method for the user account. Users login to the TOE by entering their username/password credentials on the Operation Panel, the WIM login screen, or through a client's print driver or fax driver that has been configured to submit user credentials.

40 When users enter their passwords on the Operation Panel, the WIM login, or through a client's print driver or fax driver the TOE displays a sequence of dummy characters whose length is the same as that of the entered password.

41 All users accessing the TOE user interfaces are identified and authenticated before they are allowed access. Only the following functions are accessible before the user is authenticated:

a) Viewing user job lists, WIM Help, system status, the counter and information of inquiries.

b) Creation of fax reception jobs.

c) Creation of print jobs

42 The TOE authenticates users by checking the entered username/passwords credentials against the local user database or against an external authentication service (LDAP).

43 An available functions list that identifies the basic hardcopy functions a user is permitted to perform is associated with each Normal User. After successful login, users are authorized to perform functions according to their assigned user role (Normal User, MFP Administrator, or MFP Supervisor). If login fails, the user is not denied access to all functions that require user authentication.

6.2.2 FIA_PMG_EXT.1

44 For authentication within the TOE, login passwords for users can be registered only if these passwords meet the conditions specified by the selections in FIA_PMG_EXT.1.

6.2.3 FIA_AFL.1 & FTA_SSL.3

45 The TOE counts consecutive login failures for a given login name and locks out that user after an administrator-configured number of authentication failures attempts have been reached. For the U.NORMAL users, the account lockout is released when the configured lockout time has elapsed or by direct release operation performed by the MFP administrator. For the U.ADMIN users, the account lockout is released when the configured lockout time has elapsed, or by direct release operation performed by the MFP Administrator or MFP Supervisor, or by elapse of a given time after the TOE restarts.

46 The TOE can terminate user sessions at the various interfaces as follow:

a) **Operation Panel**: the user is logged out of the TOE when inactivity reaches the Operation Panel auto logout time (settable from 10 to 999 seconds).

b) **WIM**: the user is logged out of the TOE when inactivity reaches the WIM auto logout time (settable from 3 to 60 minutes).

c) **Printer driver**: the user is logged out of the TOE immediately after receiving the print data from the printer driver.

d) **Fax driver**: the user is logged out of the TOE immediately after receiving the transmission information from the fax driver.

6.2.4 FIA_X509_EXT.1

47 The TOE's X.509 certificate validation is performed either during the IPSec peer authentication process, or upon loading the certificates into the trust store. For each certificate, the TOE performs these validation steps:

a) If the certificate ‘notAfter’ date is in the past, then this is an expired certificate which is considered invalid;

b) The certificate chain must terminate with a trusted CA certificate;

c) The TOE validates a certificate path and treats a certificate as a CA certificate when certificates include the basicConstraints extensions and that the CA flag is set to “TRUE” for all CA certificates.

d) When the TOE cannot establish a connection to determine the validity of a certificate, the TOE rejects the certificate.

48 Certificate revocation checking for the above scenarios is performed using OCSP.

49 X.509 certificates are not used for trusted updates, firmware integrity self-tests or client authentication. There are no cases where the TOE acts as a TLS client, therefore the code-signing and clientAuthentication purpose is not checked in the extendedKeyUsage for related certificates.

50 The TOE ensures that the X.509 certificates adhere to RFC 5280 Section 6.3 (certificate validation and certificate path validation), which can be summarized as follows:

a) The public key algorithm and parameters are checked

b) The current date/time is checked against the validity period revocation status is checked

c) Issuer name of X matches the subject name of X+1

d) Name constraints are checked

e) Policy OIDs are checked

f) Policy constraints are checked; issuers are ensured to have CA signing bits

g) Path length is checked

h) Critical extensions are processed

51 If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted.

6.2.5 FIA_X509_EXT.2

52 The TOE uses x509 certificate authentication for IPsec.

53 The TOE has a trust store where root CA and intermediate CA certificates can be stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope.

54 Instructions for configuring the trusted IT entities to supply appropriate X.509 certificates are captured in the guidance documents.

55 In received certificates, the DN must be present and is used as the presented identifier. As part of the verification process, an OCSP responder is used to determine whether the certificate is revoked or not. If the OCSP connection cannot be established, the validation will fail and the certificate is not accepted.

6.2.6 FIA_X509_EXT.3

56 The TOE generates Certificate Requests that provide public key, Common Name, Organization, Organizational Unit and Country information.

57 The TOE validates the chain of certificates from the Root CA when receiving the CA Certificate Response.

6.3 Access Control

6.3.1 FDP_ACC.1 & FDP_ACF.1

58 The TOE controls user operations for document data and user jobs as specified in Table 18 and Table 19.

6.3.1.1 Access control rule on document data

59 The TOE provides users with the ability to perform operations on document data that are stored in the TOE.

60 Normal Users are permitted to operate on document data if the ID of the user corresponds to the Document User List for that document (i.e., the user is the "Job Owner"). A Normal User is not permitted to operate on document data for which it is not the Job Owner.

61 A Normal User who is a Job Owner may print, send by fax, send by e-mail as attachments, and delete stored documents, using the Operation Panel or a web browser.

62 The TOE allows only the Job Owner to view and delete the document data handled as a user job while Printer Function is being used.

63 While no interface to change job owners is provided, an interface to cancel user jobs is provided. If a user job is cancelled, any document the cancelled job operates will be deleted.

Table 24: Stored Documents Access Control Rules for Normal Users

Function	User interface	Type of document	Operations permitted for authorized users
Printer	Operation Panel	+PRT	Print Delete
Printer	Web browser	+PRT	Delete
Scanner	Operation Panel	+SCN	E-mail transmission
Fax	Operation Panel	+FAXIN	Print Delete
Document Server	Operation Panel	+DSR	Print Delete
Document Server	Web browser	+DSR	Delete

64 MFP Administrators are not permitted to print, download, or send stored documents. MFP Administrators may delete stored documents, using the Operation Panel, web browser, or indirectly by cancelling a job.

65 The MFP Supervisor is not permitted to perform any document operations.

6.3.1.2 Access control rule on user jobs

66 The TOE displays on the Operation Panel a menu to cancel a user job only if the user who logs in from the Operation Panel is a Job Owner or MFP Administrator and a cancellation of a user job is attempted by the Job Owner or an MFP Administrator. Other users are not allowed to operate user jobs.

67 When a user job is cancelled, any documents operated by the cancelled job will be deleted. However, if the document data operated by the cancelled user job is a stored document, the data will not be deleted and remain stored in the TOE.

6.4 Cryptographic Operations

6.4.1 FCS_CKM.1/AKG, FCS_CKM.1/SKG, FCS_RBG_EXT.1

68 The TOE implements random-bit generation services using a software based DRBG that has been seeded with at least 256-bits of entropy from a third-party hardware-based TRNG and DRBG.

Table 25: Random Number Sources

RNG	Method	Standard	RNG
Hardware TRNG + DRBG	True RNG Hash_DRBG_SHA256	AIS31 Class 2 SP 800-90A	Hardware TRNG Firmware DRBG
Software DRBG	Hash_DRBG_SHA256 CTR_DRBG (AES-256)	SP 800-90A	Software DRBG

69 The TOE generates the following cryptographic keys in support of secure communications:

a) FFC DH Groups 14

b) RSA 2048, 4096 bits

c) ECDHE P-256, P-384 and P-521.

d) 128-bit, 192-bit (for IPsec only) and 256-bit symmetric keys

70 Additional details about key creation, the TRNG, and the DRBG, are provided in the Key Management Description and Entropy Description documents.

71 FCS_CKM.1.1/AKG meets RFC 3526 and 7919 requirements through implementation of FFC schemes using DH Group 14 (2048-bit MODP) for IPSec and DHE-2048 (ffdhe2048) for TLS, with standardized safe-prime parameters. The TOE does not generate these prime groups but correctly uses the predefined parameters from the RFCs while generating the private values using NIST-compliant DRBGs (CTR_DRBG: AES-256) for IPSec and wolfCrypt library's Hash_DRBG (SHA-256) for TLS, seeded with sufficient entropy. This approach ensures secure asymmetric key generation for protocols like IKE/IPsec in accordance with the standards specified in the SFR.

72 The TOE invokes FCS_RBG_EXT.1 functionality through standardized cryptographic library calls during key generation processes. When cryptographic keys are required, the TOE's key generation functions invoke the appropriate DRBG implementation (Hash_DRBG or CTR_DRBG) through established API interfaces. These DRBGs obtain their seed material from the hardware-based entropy source through the operating system's random number interface, ensuring that all key

generation operations comply with FCS_RBG_EXT.1 requirements for sufficient entropy.

6.4.2 FPT_SKP_EXT.1, FCS_CKM.4 and FCS_CKM_EXT.4

73 All pre-shared keys, symmetric keys, and private keys are protected in storage and are not accessible to any user through TOE interfaces. A root encryption key is securely stored in IcKey (a Trusted Platform Module). No other plaintext keys are stored in non-volatile storage. The root encryption key is used to decrypt a key encryption key which is used to decrypt symmetric keys for encrypted storage and the Device Certificate. The IPsec PSK is stored in an encrypted partition of NVRAM.

74 The TOE's firmware uses a device driver to interacts with the underlying platform (TPM) to manage and destroy cryptographic keys in compliance with the platform's security policies.

75 The TOE destroys cryptographic keys and key materials when no longer needed. TLS and IPsec session keys are no longer needed at the end of a communication session. Private keys are no longer needed when a new certificate replaces the current device certificate. The REK, KEK, and DevCert Key are always needed and are never destroyed in the evaluated configuration. Cryptographic keys and key materials stored by the TOE can be destroyed by overwriting the key with the value of a new key.

76 When cryptographic keys are no longer needed, the TOE implements key destruction through multiple methods as outlined in the KMD. For keys in volatile memory (such as TLS session keys), the TOE destroys them at the end of the communication session and ensures complete removal when power is removed from memory. For keys in non-volatile storage (NAND Flash), the TOE destroys them by logically overwriting the previous keys with newly created keys. The TOE interacts with the TPM through its device driver to manage protected keys like the REK, which is only replaced during a Purge Data operation. This multi-layered approach ensures different key types receive appropriate destruction methods based on their storage location and usage, effectively rendering all plaintext keys and cryptographic security parameters inaccessible when no longer needed.

77 There are no scenarios or configurations where the TOE deviates from not strictly conforming to the key destruction requirement.

78 Key destruction is further described in the separate proprietary Key Management Document (KMD).

6.5 Stored Data Encryption

6.5.1 FCS_KYC_EXT.1, FPT_KYP_EXT.1, FCS_COP.1/StorageEncryption, and FCS_COP.1/KeyEnc

79 The TOE encrypts data on the SSD and in NVRAM. The keychain for encrypting field-replaceable non-volatile storage devices begins with a common Root Encryption Key (REK). The plaintext REK is stored in a hardware security module, Ic Key.

80 The REK is used to encrypt and decrypt a Key Encryption Key (KEK). The KEK is used to encrypt and decrypt Device Certificate Keys and Device Encryption Keys (DEKs) for the SSD and NVRAM. All such operations use 256-bit AES keys to protect 256-bit AES data encryption on the target devices.

Table 26: Keychain encryption

Key	En/decrypts	Algorithm	Length	SFR
Root Encryption Key (REK)	Key Encryption Key	AES CBC	256	FCS_COP.1/KeyEnc
Key Encryption Key (KEK)	Storage Key NVRAM Key DevCert Key	AES CBC	256	FCS_COP.1/KeyEnc

81 Additional details about the keychain and device encryption are provided in the Key Management Description.

6.5.2 FDP_DSK_EXT.1

82 Two field-replaceable non-volatile storage devices employ encryption: the SSD, and NVRAM.

83 All SSD data is encrypted with AES 256 CBC encryption by a hardware component, Ic Ctrl. SSD encryption is enabled and initialized in the evaluated configuration, as described in the guidance documentation.

84 NVRAM is divided into encrypted and plaintext areas. Encryption is provided by the GW Linux NVRAM Encryption Library using AES 256 CBC. NVRAM encryption is enabled at TOE initialization by the administrator in conjunction with storage encryption. It can also be disabled, in this case, encrypted NVRAM data is decrypted and retained in plaintext. Other area of NVRAM do not contain confidential User or TSF Data.

85 Keychain, key management, and other details are provided in the Key Management Description.

6.6 Protection of the TSF

6.6.1 FPT_STM.1

86 The date (year/month/day) and time (hour/minute/second) the TOE records for the audit log are derived from the system clock of the TOE. The system clock is also used for other time-related functions, including user lockout timing, idle session timeouts, and SA lifetimes.

87 The system clock may be set locally or configured to use a network time server. Only an MFP Administrator can configure the system clock.

6.6.2 FPT_SBT_EXT.1

88 The TOE uses hash and digital signature verification method to confirm integrity of its firmware/software. The TPM is initialized during TOE manufacturing. The BIOS calculates the hash values of the BIOS itself, the GPT, and the bootloader, registers them into the TPM, and invokes the bootloader. The bootloader calculates the hash value of the kernel/initrd, registers it into the TPM, and invokes the kernel. The kernel/initrd calculates the hash value of system.mod, registers it into the TPM, and invokes the platform module in system.mod.

89 The module integrity verification (signature verification) is performed using the Ricoh Cryptographic Library for IMA. If verification fails, it is retried up to once by restoring the signature using libimaevm. The signature source data comes from a file (the signature by the vendor) that has already been verified during firmware update. This signature source data is also signed by IMA, and its integrity is verified prior to restoring the signature. If an integrity verification error occurs in the source data, the signature will not be restored. If any errors occur during integrity verification of modules (including retries) or integrity verification of signature source data, a service call is issued, and the system stops.

90 As mentioned, if any of the hash values differ from the expected hash values registered in the TPM, a service call is issued, and the system is stopped. The basic system part, consisting of the kernel and the platform module, cannot access the storage encryption area or invoke other modules without the storage key and Integrity Measurement Architecture (IMA) key. If all values match, the system proceeds to verify other modules using the IMA public key (RSA-2048) decrypted with KEK, instead of verifying hash values with the TPM. Note that, the KEK itself is first decrypted using the REK that is released from the TPM.

91 The Smart Operation Panel (SOP) software operates independently from the Controller. The boot process for SOP begins with the SoC ROM-based bootloader loading and executing the eMMC bootloader, which then loads and executes U-Boot, enabling write-protection of the eMMC Boot Partition. The VBMeta image’s signature is validated using the RSA and SHA256 Modules for U-Boot; if validation fails, the boot process halts and LEDs blink to indicate failure. If successful, the SHA256 Module for U-Boot validates the Kernel code against the VBMeta data using hash validation; hash validation failure results in a halted boot process and blinking LEDs, while successful validation leads to the kernel being loaded and executed. Finally, the kernel validates the Android-like OS and firmware against the VBMeta data using SHA256 hash validation from the Ricoh Cryptographic Library for Linux Kernel; failure halts the boot process with blinking LEDs, while success mounts and begins execution of the OS and firmware.

92 The Root of Trust's immutability is ensured through multiple hardware protection mechanisms: the TPM's tamper-resistant hardware design that securely stores the Root Encryption Key (REK) in protected non-volatile storage, the SoC's eFUSE (one-time programmable) that prevents BIOS modification; and SoC ROM-based bootloaders that cannot be altered. Access to the REK is strictly controlled by the TPM's Platform Configuration Registers (PCRs) during the boot process. For the Smart Operation Panel, additional protection is provided through eMMC write-protection enabled early in the boot process (which, once set, cannot be changed until the next power cycle). This multi-layered approach creates a hardware-anchored trust chain where the TPM's design prevents unauthorized modification of both the REK and PCR measurements, while the manufacturing initialization process establishes this root in a controlled environment.

93 For additional details of the key contained in the Root of Trust refer to the Key Management Description (KMD) document.

6.7 Trusted Communications

94 The Trusted Communications Function provides trusted paths for communications between the TOE and remote users / external IT entities.

6.7.1 FTP_TRP.1/Admin, FTP_TRP.1/NonAdmin, FCS_HTTPS_EXT.1, FTP_ITC.1 and FCS_TLSS_EXT.1

95 The TOE implements TLS 1.2 to protect communications between the TOE and remote users' client computers (print drivers, fax drivers, and WIM HTTPS sessions). TLS client authentication is not supported.

96 The TOE supports the following ciphersuites when it acts as a TLS server:

a) TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256

b) TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256

c) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

d) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

e) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

f) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

97 For TLSS, The TOE implements TLS 1.2 in compliance with RFC 5246.

98 The TOE denies all TLS connection attempts using SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 through administrative configuration.

99 The TOE supports session resumption through the use of session IDs according to RFC 5246. Session resumption is protected using AES 128 CBC, AES 256 CBC, AES 128 GCM or AES 256 GCM.

100 The TOE Web Image Monitor (WIM) is accessed via an HTTPS connection using TLS implementation as described above. The TOE does not use HTTPS in a client capacity. The TOE's HTTPS protocol complies with RFC 2818.

101 RFC 2818 specifies HTTP over TLS. The majority of RFC 2818 is spent on discussing practices for validating endpoint identities and how connections must be setup and torn down. The TOE's WIM GUI operates on an explicit port designated to natively utilizes TLS for communication as described in section 2.3 of RFC 2818. After successful handshake, all HTTP data transmit as TLS application data as per section 2.1 of RFC 2818. The WIM attempts to send closure Alerts prior to closing a connection in accordance with section 2.2.2 of RFC 2818.

6.7.2 FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_CKM.2, FCS_TLSS_EXT.1, and FCS_COP.1/KeyedHash

102 The TOE supports RSA signature generation and verification in accordance with FIPS PUB 186-4. Specifically, the TOE generates a self-signed RSA Device Certificates using key sizes of 2048-bits or 4096-bits. Administrators may import a Device Certificate that is generated outside of the TOE.

103 To establish a session key for TLS communications, the TOE employs a Diffie-Hellman-based key establishment scheme conforming to NIST SP 800-56A Section 5.6, and a Hash DRBG.

104 The TOE provides keyed-hash message authentication in accordance with ISO/IEC 9797-2:2011, Section 7 using, HMAC-SHA-256, or HMAC-SHA-384. The HMAC function uses the following values:

- Key Length: 512 or 1024 bits
- Hash Function: SHA-256, SHA-384
- Block Size: 512 bits for HMAC-SHA-256 and 1024 bits for HMAC-SHA-384

- Output MAC Length: 256 bits for HMAC-SHA-256, 384 bits for HMAC-SHA-384

105 The session key is used to encrypt communications with AES 128 CBC, AES 256 CBC, AES 128 GCM or AES 256 GCM.

Table 27: TLS/HTTPS Cryptographic Functions

Function	SFR	Algorithm
Key Generation	FCS_CKM.1/AKG	ECDSA Key Generation Curve (P-256, P-384, P-521) ECDSA Key Verification Curve (P-256, P-384, P-521)
Key Establishment	FCS_CKM.2	KAS-FFC-SSC (DHE) KAS-ECC-SSC (ECDHE)
Signature Generation and Verification	FCS_COP.1/SigGen	RSA (2048, 4096 bits)
Random Bit Generation	FCS_RBG_EXT.1	Hash_DRBG_SHA256
Encryption / Decryption	FCS_COP.1/DataEncryption	AES 128 CBC AES 256 CBC AES 128 GCM AES 256 GCM
Keyed-Hash Message Authentication	FCS_COP.1/KeyedHash	HMAC-SHA-256 HMAC-SHA-384

6.7.3 FTP_ITC.1, FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, FCS_COP.1/DataEncryption, FCS_COP.1/Hash, and FCS_COP.1/KeyedHash

106 The TOE employs IPsec to protect communications between the TOE and external IT entities in the operational environment. In the evaluated configuration, it is used for communications with LDAP, syslog, NTP, SMTP, and FTP servers.

107 IPsec is operated in transport mode or tunnel mode, as set by the administrator.

108 IPsec supports automatic key exchange by IKEv1.

109 In Phase 1, peer authentication supports two types of authentication: pre-shared key authentication and digital certificate authentication.

110 The pre-shared key can be any length from 1 to 32 characters, and is composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”). Text-based pre-shared keys of 22 characters is supported. The pre-shared key is configurable with an ASCII text string, and it is conditioned using the same algorithm that is selected for the Phase 1 hash algorithm: SHA-256, SHA-384 or SHA-512.

111 An administrator can select whether to use main mode or aggressive mode. In the evaluated configuration, only main mode is used.

112 In IKEv1, the TOE supports DH Group 14. The security strength associated with the DH Group 14 is 112 bits as defined in NIST SP 800-57 Rev. 5 “Recommendation for Key Management –Part 1: General”. The TOE allows an administrator to specify this DH group to be used for IKE session establishment.

113 IKEv1 key lifetimes can be set by the administrator, from 300 seconds to 172,800 seconds. In the evaluated configuration, Phase 1 key lifetime is set to 86,400 seconds (24 hours), and Phase 2 lifetime is set to 28,800 seconds (8 hours).

114 Supported encryption algorithms for IKE and ESP are AES-128-CBC, AES-192-CBC, and AES-256-CBC. AES-128-CBC may only be used if IKE negotiation also at least selects AES-128-CBC.

115 The TOE supports keyed-hash algorithms HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 to ensure message integrity and authenticity. Additionally, the TOE does not utilise a truncated version of the SHA-based HMAC functions.

116 As an SPD, four individual entries and one default entry of “Apply” can be set by an administrator. Beginning with the first entry, the packet is compared, and if it matches the entry, IPsec communication is performed. If the packet does not match the first entry, subsequent entries are tested until there is a match. If no entries match the packet, the default entry will be compared and applied. In the TOE configuration, the default rule is "Discard".

117 The TOE generates the secret value "x" used in IKE Diffie-Hellman key exchange using the random bit generator specified in FCS_RBG_EXT.1. The TOE generates "x" with a minimum length of 224 bits for all supported DH groups:

- Group 14 (2048-bit MODP) according to RFC 3526

118 The "x" value is generated at the start of each IKE communication session using approved cryptographic methods. This ensures that the private value "x" has sufficient randomness and meets the length requirements for secure Diffie-Hellman key exchange in IKE protocols.

119 The TOE generates nonces used in IKEv1 exchanges using the random bit generator specified in FCS_RBG_EXT.1. The nonce generation process ensures compliance with the following FCS_IPSEC_EXT.1.10 requirements:

- Nonces are generated with a length of at least 128 bits
- Nonces are generated with a length of at least half the output size of the negotiated pseudorandom function (PRF) hash

120 The TOE supports the following PRF hash functions with corresponding minimum nonce lengths: SHA-256: minimum 128 bits, SHA-384: minimum 192 bits, and SHA-512: minimum 256 bits.

121 The nonce generation uses approved cryptographic methods and applies to the IKEv1 implementation and supported DH Group, ensuring sufficient randomness for secure IKE exchanges.

122 During IKEv1 Phase 2 CHILD_SA suite negotiations, the TOE ensures that the symmetric algorithm key strength (in bits) selected for Phase 2/CHILD_SA does not exceed the key strength of the established Phase 1/IKE_SA. The TOE enforces this strength validation by default, maintaining the security hierarchy where the protecting SA (Phase 1/IKE_SA) has strength greater than or equal to the protected SA (Phase 2/CHILD_SA).

123 The TOE supports the following cryptographic algorithms:

Table 28: IPsec Cryptographic Functions

Function	SFR	Algorithm
IKEv1	FCS_CKM.1/AKG FCS_CKM.1/SKG FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	KAS-FFC RSA 186-4 AES 128 CBC AES 192 CBC AES 256 CBC SHA-256 SHA-384 SHA-512 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 CTR_DRBG(AES-256)
ESP	FCS_COP.1/DataEncryption FCS_COP.1/KeyedHash FCS_RBG_EXT.1	AES 128 CBC AES 192 CBC AES 256 CBC HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 CTR_DRBG(AES-256)

6.8 Administrative Roles

124 The Security Management Function consists of functions to 1) control operations for TSF data, 2) maintain user roles assigned to Normal Users, MFP Administrator, or MFP Supervisor to operate the Security Management Function, and 3) set appropriate default values to security attributes, all of which accord with user role privileges or user privileges that are assigned to Normal Users, MFP Administrator, or MFP Supervisor.

6.8.1 FMT_SMR.1

125 The TOE maintains U.NORMAL and U.ADMIN roles as described in Table 6. U.NORMAL defines the normal or non-admin users of the TOE which are permitted to use the document processing functions of the MFP and access their own data. U.ADMIN defines all TOE administrators, which includes the MFP Administrator and the MFP Supervisor. The MFP Administrator configures the TOE, manages normal users' jobs and normal users' data. The MFP supervisor sets MFP Administrators' passwords. Administrators do not initiate document processing jobs.

6.8.2 FMT_SMF.1, FMT_MOF.1, and FMT_MTD.1

126 The TOE provides and restricts the following management functions which can be managed over the Operation Panel or the WIM:

a) Manage user accounts including create, modify, and delete users, user roles, privileges, available function lists, and unlocking locked user accounts.

b) Manage the audit functions including enable/disable the audit functions and modifying the audit transfer settings

c) Query, delete and export the audit logs

d) Configure time and date settings

e) Password Management configuration including minimum password length, and password complexity

f) Configure auto logout time settings on WIM and the Operation Panel

g) Configure Authentication Failure and Account lockout timer settings

h) Modify PSTN Fax-Line Separation Stored Reception File User

i) Configure network settings for trusted communications (specify IP addresses and port to connect to the TOE)

j) Manage storage key, including create, delete, and modify keys

k) Manage device certificates including create, delete, modify, upload certificates

Note. Uploading device certificates is only available through the WIM.

l) Manage CA certificates including import and delete certificates

m) Manage TOE trusted update

n) Configure NTP

o) Configure SMTP over IPsec

p) Configure syslog over IPsec

q) Configure TLS

127 The TOE restricts modification of TSF functions and TSF data to the authorized administrator roles.

6.8.3 FMT_MSA.1 and FMT_MSA.3

128 Table 18 and Table 19 list the access control rules enforced by the TOE when users access the document processing functions (print, scan, copy, fax) and individual user jobs. The default behaviour to access the document data is permissive for all authenticated normal users, except for the U.ADMIN user which cannot initiate document processing functions. The TOE maintains a username and available functions list for individual users. Unauthenticated users sending print or fax jobs to the TOE must be identified before the TOE processes the job.

6.9 Trusted Operation

129 The Software Verification Function is to verify the integrity of the executable codes of the MFP Control Software, FCU Control Software and Operation Panel Control Software, and confirm that these codes can be trusted.

6.9.1 FPT_TST_EXT.1

130 During start-up, the TOE performs a series of integrity tests, that check that the hash on the executable files is correct and that the software has not been changed. The integrity tests check the hash on the software executable MFP Control Software and Operation Panel Software.

131 The module integrity verification (signature verification) is performed using the Ricoh Cryptographic Library for IMA. If verification fails, it is retried up to once by restoring the signature using libimaevm. The signature source data comes from a file (the signature by the vendor) that has already been verified during firmware update. This signature source data is also signed by IMA, and its integrity is verified prior to restoring the signature. If an integrity verification error occurs in the source data, the signature will not be restored. If any errors occur during integrity verification of modules (including retries) or integrity verification of signature source data, a service call is issued, and the system stops.

132 As mentioned, if any of the hash values differ from the expected hash values registered in the TPM, a service call is issued, and the system is stopped. The basic system part, consisting of the kernel and the platform module, cannot access the storage encryption area or invoke other modules without the storage key and Integrity Measurement Architecture (IMA) key. If all values match, the system proceeds to verify other modules using the IMA public key (RSA-2048) decrypted with KEK, instead of verifying hash values with the TPM. Note that, the KEK itself is first decrypted using the REK that is released from the TPM. When all steps succeed, the TOE becomes operational.

133 The Smart Operation Panel (SOP) software operates independently from the Controller. The boot process for SOP begins with the SoC ROM-based bootloader loading and executing the eMMC bootloader, which then loads and executes U-Boot, enabling write-protection of the eMMC Boot Partition. The VBMeta image's signature is validated using the RSA 4096-bit and SHA256 Modules for U-Boot; if validation fails, the boot process halts and LEDs blink to indicate failure. If successful, the SHA256 Module for U-Boot validates the Kernel code against the VBMeta data. A hash validation failure results in a halted boot process and blinking LEDs, while successful validation leads to the kernel being loaded and executed. Finally, the kernel validates the OS and firmware against the VBMeta data using SHA256 from the Ricoh Cryptographic Library for Linux Kernel. Failure of this validation halts the boot process with blinking LEDs, while a successful validation mounts and begins execution of the OS and firmware.

134 The TOE outputs information for verifying the integrity of the FCU Control Software. This information can be compared with guidance documents to ensure the integrity of the FCU Control Software.

135 The integrity tests described above constitute the complete set of self-tests performed during TOE startup.

6.9.2 FPT_TUD_EXT.1

136 TOE allows only the MFP Administrator to read the version of the MFP Control Software, Operation Panel Control Software, and Operation Panel Applications. The MFP Administrator can read these versions using the Operation Panel or WIM from the client computer.

137 The MFP Administrator can prepare for installation of updated MFP Control Software, Operation Panel Software, or Operation Panel Applications, by uploading an installation package from the client computer using WIM. The package contains the TOE Software and a digital signature (DS) that was created using the SERES

private key. Digital signatures for trusted updates are generated outside of the TOE, by the manufacturer.

138 For MFP Control or Operation Panel Software, the TOE performs the following verifications before the installing the package:

a) Identifies the type of software (e.g., MFP Control, Operation Panel);

b) Verifies that the software model name matches the TOE;

c) Creates a SHA256 message digest (MD1) of the software, uses the SERES public key (RSA 2048-bit) to decrypt DS (MD2), and then verifies that MD1 = MD2.

139 For Operation Panel software, the TOE performs the following verifications before the installing the package:

a) Identifies the type of software (e.g., MFP Control, Operation Panel);

b) Verifies that the software model name matches the TOE;

c) Creates a SHA256 message digest (MD1) of the index file, uses the SERES public key to decrypt DS (MD2), and then verifies that MD1 = MD2.

d) Creates a SHA256 message digest (MD3) of the software image, uses an internal key to decrypt DS (MD4), and then verifies that MD3 = MD4.

140 For each Operation Panel application, the TOE performs the following verifications before the installing the package:

a) Verifies that the application is Ricoh's by checking the certificate contained in the APK.

b) Creates a SHA256 message digest (MD1) of the application, uses the public key in the certificate to decrypt DS (MD2), and then verifies that MD1 = MD2.

141 The TOE performs the signature verification of the software to be updated using the encryption functions listed below when updating the software.

Table 29: Signature Verification

Integrity test	SFR	Algorithm
MFP Control Software	FCS_COP.1/SigGen FCS_COP.1/Hash	RSA 186-4 SHA-256
Operation Panel Software	FCS_COP.1/SigGen FCS_COP.1/Hash	RSA 186-4 SHA-256
Operation Panel Applications	FCS_COP.1/SigGen FCS_COP.1/Hash	RSA 186-4 SHA-256

6.10 PSTN Fax-Network Separation

142 The Fax Line Separation Function permits only fax transmissions as input information from telephone lines so that unauthorized intrusion from telephone lines can be prevented.

6.10.1 FDP_FXS_EXT.1

143 The fax interface use cases are below.

a) Sending faxes

i) The TOE receives documents from client PCs via the LAN, and using the fax interface, transmits them as fax documents via the PSTN line using the ITU-T T.30 protocol.

ii) The TOE can transmit stored documents as faxes.

b) Receiving faxes

i) A remote fax machine establishes a connection to the TOE through the PSTN line using the ITU-T T.30 protocol, through which the TOE receives fax documents.

c) Fax-Line Separation

i) The fax modem accepts connections through the PSTN only if they conform to the ITU-T T.30 protocol.

ii) Data that is transmitted or received through the PSTN is fax-format, image data.

144 Other than the specified use cases, the TOE allows no other data to be transmitted on the fax line.

7 Rationale

7.1 Conformance Claim Rationale

145 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is hardcopy device, consistent with the HCDcPP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the HCDcPP.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the HCDcPP.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced directly from the HCDcPP. No additional requirements have been specified.

7.2 Security Objectives Rationale

146 The following table maps all threats, OSPs, and assumptions to their respective Security Objectives, and is reproduced from HCDcPP Appendix I.8.

Table 30: Security Objectives Rationale

Threat/Policy/Assumptions	Rationale
T.UNAUTHORIZED_ACCESS An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.	O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators. O.AUTH_FAILURES resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.
T.TSF_COMPROMISE An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.	O.ACCESS_ CONTROL restricts access to TSF Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_FAILURE	O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected.

Threat/Policy/Assumptions	Rationale
A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.	
T.WEAK_CRYPTO An attacker may exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes.	O.STRONG_CRYPTO implements strong cryptographic mechanisms to provide sufficient resistance to current attack capabilities.
T.UNAUTHORIZED_UPDATE An attacker may cause the installation of unauthorized firmware/software on the TOE.	O.UPDATE_VERIFICATION verifies the authenticity of firmware/software updates.
T.NET_COMPROMISE An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.	O.COMMS_PROTECTION protects LAN communications from sniffing, replay, and man-in-the-middle attacks.
P.AUTHORIZATION Users must be authorized before performing Document Processing and administrative functions.	O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users. O.USER_I&A provides the basis for authorization. O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators.
P.AUDIT Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.	O.AUDIT requires the generation of audit data. O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users. O.USER_AUTHORIZATION provides the basis for authorization.
P.COMMS_PROTECTION The TOE must be able to identify itself to other devices on the LAN.	O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks.
P.STORAGE_ENCRYPTION If the TOE stores User Document Data or Confidential TSF Data on Nonvolatile Storage Devices, it will encrypt such data on those devices and the TOE shall provide a function that an authorized administrator may destroy encryption keys or keying material when the TOE is removed from its Operational Environment or its ownership is changed.	O.STORAGE_ENCRYPTION protects User Document Data or Confidential TSF Data stored in Nonvolatile Storage Devices from exposure if a device has been removed from the TOE and its Operational Environment.

Threat/Policy/Assumptions	Rationale
P.KEY_MATERIAL Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.	O.KEY_MATERIAL protects keys and key materials from unauthorized access and ensures that they any key materials are not stored in cleartext on the device that uses those materials for its own encryption.
P.FAX_FLOW (conditionally mandatory) If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.	O.FAX_NET_SEPARATION requires a separation between the PSTN fax line and the LAN.
P.ROT_INTEGRITY The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters.	O.FW_INTEGRITY ensures that the TOE's own integrity remains intact and can attest its integrity to outside parties on request.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.	OE.PHYSICAL_PROTECTION establishes a protected physical environment for the TOE.
A.NETWORK The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.	OE.NETWORK_PROTECTION establishes a protected LAN environment for the TOE.
A.TRUSTED_ADMIN TOE Administrators are trusted to administer the TOE according to site security policies.	OE.ADMIN_TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.TRAINED_USERS Authorized Users are trained to use the TOE according to site security policies.	OE.ADMIN_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Administrators. OE.USER_TRAINING ensures that Users are aware of site security policies and have the competence to follow them.

7.3 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 cPP are used to provide tailored guidance on the specific expectations for completing the security assurance requirements.