Xerox® VersaLink™ C415 / B415 / C625 / B625 with eMMC

Security Target

Version 1.0

March 2026

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
1.0	05 Mar 2026	Release for certification.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Xerox® VersaLink™ C415 / B415 / C625 / B625 with eMMC Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE is a hardcopy device that copies and prints with scan and fax capabilities.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Xerox® VersaLink™ C415 / B415 / C625 / B625 with eMMC
Security Target	Xerox® VersaLink™ C415 / B415 / C625 / B625 with eMMC Security Target, v1.0

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	Source	Applicability Rationale
TD0926	HIT Technical Decision: Clarification on FPT_SBT_EXT.1 Root of Trust	CPP_HCD_V1.0E	Applicable.
TD0927	HIT Technical Decision: Clarification on FPT_KYP_EXT.1 when using TPM-like device	CPP_HCD_V1.0E	Applicable.
TD0996	CPP_HCD_V1.0 Endorsement Requirements	CPP_HCD_V1.0E	Applicable.
TD0997	HIT Technical Decision: FCS_SSHC_EXT.1.8 and FCS_SSHS_EXT.1.8 Time based test case as optional	CPP_HCD_V1.0E	Applicable.

TD #	Name	Source	Applicability Rationale
TD0998	HIT Technical Decision: Remove FCS_CKM.1/SKG dependency of FCS_COP.1/CMAC when used in Secure Boot	CPP_HCD_V1.0E	Not applicable. FCS_COP.1/CMAC is not claimed.
TD0999	HIT Decision: Permit use of FIPS 186-5 Digital Signature Standard algorithms in FCS_COP.1/SigGen	CPP_HCD_V1.0E	Applicable.
TD1000	HIT Technical Decision: Remove TSS assurance activities from the Tests section	CPP_HCD_V1.0E	Applicable.

1.4 Terminology

4 Terms used in this document are defined in Table 3 below and in Appendix G of the HCDcPP.

Table 3: Terminology

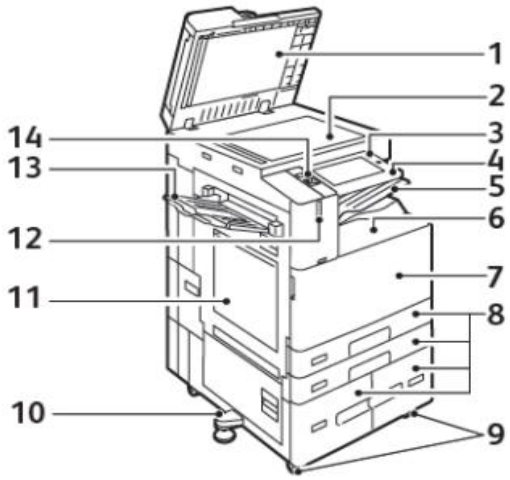
Term	Definition
BEV	Border Encryption Value
CC	Common Criteria
Control Panel	Also referred to as the ‘Local UI’. A local user interface on the MFD.
DEK	Data Encryption Key
EAL	Evaluation Assurance Level
eMMC	Embedded Multi Media Card
EWS	Embedded Web Server, also referred to as the ‘WebUI’. A web-based user interface that is part of the TOE.
HCDPP	Protection Profile for Hardcopy Devices
I&A	Identification and Authentication
KMD	Key Management Description (Xerox proprietary)
LanFax	Enables fax jobs to be submitted from the desktop via printing protocols.

Term	Definition
LUI	Local User Interface / Local UI refer to the Control Panel. These terms are used interchangeably.
MFD	Multi-Function Device
MFP	Multi-Function Printer
NVM	Non-Volatile Memory
PP	Protection Profile
PSTN	Public Switched Telephone Network
STARTTLS	A protocol command used to inform the email server that the email client wants to upgrade from an insecure connection to a secure TLS connection.
TOE	Target of Evaluation
TSF	TOE Security Functionality
IPP	Internet Printing Protocol
AirPrint	Apple's wireless printing tech for driverless printing from iOS/macOS
Mopria Discovery	Protocols that allow discovery and connection with Mopria-enabled device (like an Android phone, tablet, or Windows PC)

2 TOE Description

2.1 Deployment

5 The TOE is a hardcopy device that copies and prints with scan and fax capabilities, commonly known as Multi-Function Device (MFD), Multi-Function Printer (MFP) or simply printer.



1. Document Cover
2. Document Glass
3. Power/Wake Button
4. Near Field Communication (NFC) Area
5. Center Output Tray
6. Center Bottom Tray
7. Main Power Switch behind the front door
8. Trays 1–4
9. Locking Casters
10. Leveler Foot
11. Tray 5 – Bypass Tray
12. Smart Proximity Sensor
13. Left Tray
14. Front USB Port, Type A

Figure 1: TOE Front View

2.2 Usage

6 The TOE is deployed within office environments for general copy/print/scan/fax use by non-administrative users. The primary interface for users is the Control Panel which provides status information, allows device configuration and provides access to hardcopy functions.

7 In addition to the Control Panel, users may also interact with the TOE via the Embedded Web Server (EWS), a web-based user interface that provides status information, allows device configuration, and provides access to some hardcopy functions such as print job management and submission.

2.2.1 General Use

8 The general TOE use cases are:

a) **Copy.** Users are physically present at the device and interact via the Control Panel to produce hard copies of a source document.

b) **Print.** Users submit print jobs and physically collect hardcopy output at the printer. Print submission has the following characteristics in the evaluated configuration:

   i) **Print from User Device.** Users submit print jobs via Xerox print drivers on supported Operating Systems (see section 2.4.1). In the evaluated configuration, these print jobs are submitted over IPsec.

   ii) **Print from Mailbox.** Users may print documents/images from their Scan-to-Mailbox (see Scan to Mailbox below) via EWS or the Control Panel.

   iii) **Print from EWS.** Users may upload files for printing via EWS.

   iv) **Secure Print.** All print jobs are held until released by entering a passcode at the Control Panel (this is in addition to user authentication at the Control Panel).

c) **Scan.** Users are physically present at the printer and interact via the Control Panel to submit a scan job. The following scan destinations are supported in the evaluated configuration:

   i) **Scan to Mailbox.** Send scanned images to a unique Scan-to-Mailbox for an authenticated user. These images are stored on the TOE and may be downloaded via EWS, printed or deleted.

   ii) **Scan to Email.** Send scanned images to an email address via STARTTLS**.**

   iii) **Workflow Scanning.** Send scanned images to a Workflow Repository (file server) via HTTPS.

d) **Fax.** The TOE can be used to send and receive facsimile documents. In the evaluated configuration, the fax capability has the following characteristics:

   i) **Fax using Control Panel.** Users are physically present at the printer and interact via the Control Panel to send or receive a facsimile document.

   ii) **Fax from User Device.** Users submit fax print jobs via Xerox print drivers on supported Operating Systems (see section 2.4.1). In the evaluated configuration, fax print jobs are submitted over IPsec (user devices require an IPsec client).

   iii) **Secure Jobs.** All received fax jobs are held until released by entering a passcode at the Control Panel (this is in addition to user authentication at the Control Panel).

   iv) **Fax Forwarding.** Fax forwarding rules may be configured to send received fax jobs to email via STARTTLS.

2.2.2 Administration

9 System Administrators manage TOE configuration via the Control Panel and/or EWS.

2.2.3 Secure Communication Protocols

10 Figure 2 shows the secure communication protocols that are used by the TOE in support of general and administrative use cases.

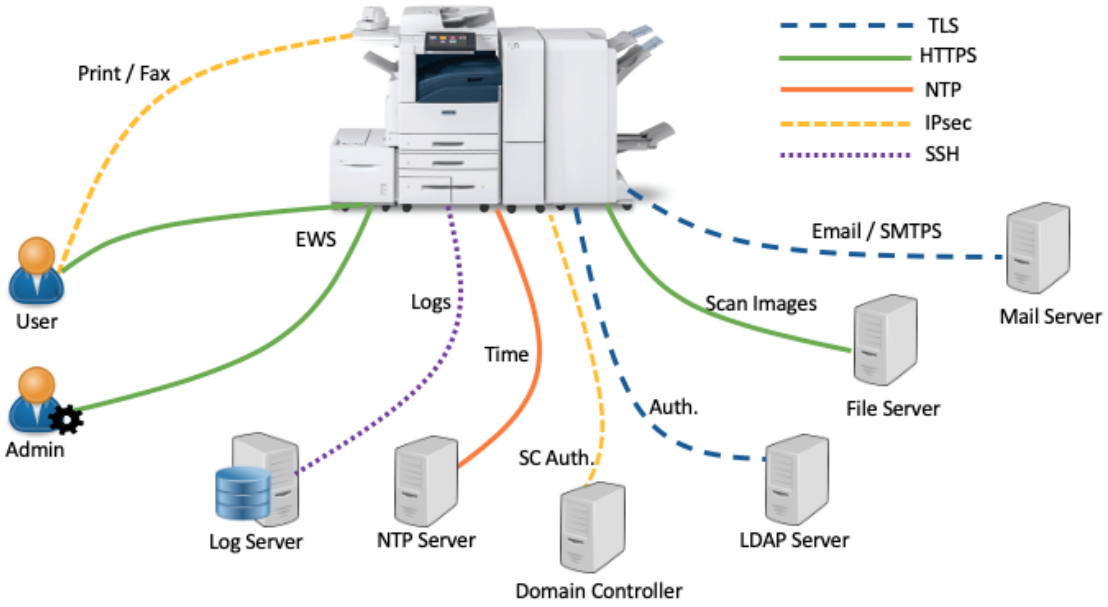


Figure 2: TOE Secure Communication

11 The TOE uses the following secure communication protocols:

a) **IPsec.** Print and fax jobs submitted from user devices are sent over IPsec. Smartcard authentication at the Control Panel makes use of an IPsec tunnel between the TOE and the Windows Domain Controller.

b) **HTTPS.** Communication between EWS and remote users occurs via HTTPS. Workflow Scanning uses HTTPS between the TOE and the Workflow Repository file server.

c) **TLS.** TLS protects communication between the TOE, LDAP servers and Mail Servers.

d) **SSH.** Transfer of log files to a remote server is protected via SSH/SFTP.

e) **NTP.** The TOE synchronizes time using NTP.

2.3 Logical Scope

12 The TOE logical scope encompasses the following security functions:

a) **Identification and Authentication.** The TOE requires users and system administrators to authenticate before granting access to printer or system administration functions via EWS or the Control Panel. The TOE supports username/password and smartcard-based authentication.

b) **Access Control.** The TOE enforces access controls to ensure that documents, information related to document processing, and security-relevant data are accessible only to users who have appropriate access permissions.

c) **Data Encryption.** The TOE stores temporary files created during a copy, print, scan and fax job in encrypted format on single storage drive. All partitions of the drive used for spooling temporary files are encrypted.

d) **Trusted Communication.** The TOE protects the integrity and confidentiality of communications as noted in section 2.2.3 above.

e) **Administrative Roles.** The TOE enforces role-based access controls to ensure that the ability to configure security settings is available only to users who have been authorized with an administrator role.

f) **Auditing.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

g) **Trusted Operation.** The TOE performs a suite of self-tests to verify correct operation during start-up and verifies the authenticity and integrity of firmware updates.

h) **PSTN Fax-Network Separation.** The TOE provides separation between the fax processing board and the network interface and therefore prevents an interconnection between the PSTN and the internal network. This separation is realized in software, as by design, these interfaces may only communicate via an intermediary.

i) **Data Clearing and Purging.** The purge feature allows an authorized administrator to permanently delete all customer-supplied data on the TOE. This addresses residual data concerns when the TOE is decommissioned from service or redeployed to a different environment.

j) **Cryptographic Operations.** The TOE incorporates two Mocana cryptographic modules that it uses for all in-scope cryptographic operations.

2.4 Physical Scope

13 The physical boundary of the TOE includes all software and hardware included in the models shown in Table 4. The TOE is delivered to the customer via commercial courier. The TOE models vary in print speeds.

14 The TOE includes an Infineon OPTIGA TPM SLB 9672 FW15, a TPM 2.0-compliant implementation with FIPS 140-2 certification. This TPM is used to securely store disk encryption keys.

15 The TOE is equipped with a factory standard eMMC flash storage device.

Table 4: TOE models

Model	Firmware Version	CPU / OS
VersaLink™ B415	122.029.005.15402	ARM Cortex A53 (ARMv8-A) Yocto Linux 3.1.24
VersaLink™ C415	122.028.005.15402	
VersaLink™ B625	122.025.005.15402	
VersaLink™ C625	122.024.005.15402	

2.4.1 Guidance Documents

16 The following guidance documentation is provided to end users in Portable Document Format (PDF) online at https://www.support.xerox.com/en-us:

a) Secure Installation and Operations Guide Xerox® VersaLink® C415/C625/B415/B625 Multifunction Printer v2.3, February 2026

b) Xerox® VersaLink® B620/C620 Printers and VersaLink® B415/C415/B625/C625 Multifunction Printers System Administrator Guide, v2.1, July 2025 (702P09390)

c) Xerox® VersaLink® C625 Color Multifunction Printer User Guide, v2.2, July 2025 (702P09381)

d) Xerox® VersaLink® B625 Multifunction Printer User Guide, v2.2, July 2025 (702P09382)

e) Xerox® VersaLink® B415 Multifunction Printer User Guide, v2.1, July 2025 (702P09386)

f) Xerox® VersaLink® C415 Color Multifunction Printer User Guide, v2.2, July 2025 (702P09385)

g) Smart Card Installation and Configuration Guide for Xerox® AltaLink® / Versalink® Series, v5.0, October 2025 (702P09502)

2.4.2 Non-TOE Components

17 The TOE operates with the following components in the environment:

a) IPv4 or IPv6 network environment

b) Publicly Switched Telephone Network (PSTN)

c) LDAP server for authentication services

d) NTP server for time services

e) File server for Workflow Scanning

f) Log server (file server) for remote log storage

g) Printer drivers on supported OS per https://www.support.xerox.com/en-us

h) Smart card authentication requires Federal Information Processing Standard (FIPS) 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smart cards and readers or equivalent. In support of smart card authentication, a Windows Domain Controller must also be present in the environment.

i) Web browser with JavaScript support (to access the EWS web GUI)

2.4.3 Functions not included in the TOE Evaluation

18 For the TOE to be in the evaluated configuration, the following functions must not be enabled/used:

a) Reprint from Saved Job

b) SMart eSolutions

c) Custom Services (Extensible Interface Platform or EIP)

d) Network Accounting and Auxiliary Access

e) Embedded Fax mailboxes

f) Wi-Fi Direct Printing
g) Weblet Services
h) InBox Apps
i) Remote Control Panel
j) SFTP when used for scanning
k) SNMPv3
l) Scan to USB
m) Print from USB
n) SMB Filing
o) Convenience Authentication
p) Xerox Workplace Cloud
q) Proximity Card Authentication
r) Remote services
s) AirPrint
t) Mopria Discovery
u) IPP

2.4.4 CAVP Certificates

19 Users can verify the CAVP certificates by comparing the Xerox module version listed in the certificate with the module version displayed when an administrator selects “device information” from the touch panel.

Table 5: CAVP certificates

Module	Algorithm(s) (keys/curves/digest-size)	Usage	CAVP
Mocana Cryptographic Library, v 7.0.0f_u1	AES-128/256 (CBC/CTR mode) RSA-2048 ECDH-P256/P384/P521 HMAC-SHA-256/512 ECDSA-P256/P384	SSH	A4653
	AES-128/256 (CBC/GCM mode) RSA-2048/3072 HMAC-SHA-256/384 SHA-256/384 ECDSA-P256/P384/P521 KAS-FFC	TLS/HTTPS	A4653, A4655

Module	Algorithm(s) (keys/curves/digest-size)	Usage	CAVP
	KAS-ECC		
	HMAC-SHA-256	Self-test (integrity)	A4653
	SHA-256 RSA-2048	signature verification (firmware update)	A4653
	SHA-256 RSA-2048	firmware integrity verification (startup)	A4653
	AES-CBC-128/256 RSA-2048/3072 ECDSA-P256/P384/P521 HMAC-SHA-256/384 KAS-FFC KAS-ECC	IPsec	A4653
	Counter DRBG (AES-256)	Random bits for key generation	A4653
Mocana Cryptographic Library, v 7.0.0f	AES-CBC-128/256 HMAC-SHA-256	IPsec (ESP)	A845
	AES-CBC/XTS-256	Disk Encryption	A845

3 Security Problem Definition

20 The Security Problem Definition is reproduced from Appendix I and section 3 of the HCDcPP.

3.1 Users

21 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. A Normal User can be a Local User or a Network User as described in Section 1.3.2, “Operational Environment
U.ADMIN	Administrator	A User who has been identified and authenticated and has an administrative role

22 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

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

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

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

3.2.1 User Data

25 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.

Designation	User Data type	Definition
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job.

26 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

3.2.2 TSF Data

27 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.

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

3.3 Threats

29 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

Identifier	Description
	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.
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

30 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

31 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.
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.WIPE_DATA (optional)	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
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

32 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.

Identifier	Description
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.
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.WIPE_DATA (optional)	The TOE provides a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
O.AUTH_FAILURES (conditionally 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.

33 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.
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

34 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 a string starting with "/" (e.g. "FCS_COP.1/Hash").

35 **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

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

- FAU_STG_EXT.1 Extended: External Audit Trail Storage
- FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
- FCS_HTTPS_EXT.1 Extended: HTTPS selected
- FCS_IPSEC_EXT.1 Extended: IPsec selected
- FCS_KYC_EXT.1 Extended Key Chaining
- FCS_RBG_EXT.1 Extended: Random Bit Generation
- FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication
- FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication
- FCS_SSHC_EXT.1 SSH Client Protocol
- FDP_DSK_EXT.1 Extended: Protection of Data on Disk
- FDP_FXS_EXT.1 Extended: Fax separation
- FIA_PMG_EXT.1 Extended: Password Management
- FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication
- FIA_X509_EXT.3 X.509 Certificate Requests
- FPT_KYP_EXT.1 Extended: Protection of Key and Key Material
- FPT_SBT_EXT.1 Extended: Secure Boot
- FPT_SKP_EXT.1 Extended: Protection of TSF Data
- FPT_TST_EXT.1 Extended: TSF testing

- FPT_TUD_EXT.1 Extended: Trusted Update
- FPT_WIPE_EXT.1 Data Wiping

5.3 Functional Requirements

Table 16: Summary of SFRs

Class	SFRs
Security Audit (FAU)	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.4 Prevention of audit data loss
	FAU_STG_EXT.1 Extended: External Audit Trail Storage
Cryptographic Support (FCS)	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 (Data Encryption/Decryption)
	FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)
	FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
	FCS_HTTPS_EXT.1 Extended: HTTPS selected
	FCS_IPSEC_EXT.1 Extended: IPsec selected

Class	SFRs
	FCS_KYC_EXT.1 Extended: Key Chaining
	FCS_RBG_EXT.1 Random Bit Generation
	FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication
	FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication
	FCS_SSHC_EXT.1 SSH Client Protocol
User Data Protection (FDP)	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
	FDP_DSK_EXT.1 Extended: Protection of Data on Disk
	FDP_FXS_EXT.1 Extended: Fax separation
Identification and Authentication (FIA)	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
Security Management (FMT)	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

Class	SFRs
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Privacy (FPR)	There are no class FPR requirements.
Protection of the TSF (FPT)	FPT_KYP_EXT.1 Extended: Protection of Key and Key Material
	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
	FPT_TUD_EXT.1 Extended: Trusted Update
	FPT_WIPE_EXT.1 Data Wiping
Resource Utilization (FRU)	There are no class FRU requirements.
TOE Access (FTA)	FTA_SSL.3 TSF-initiated termination
Trusted Paths/Channels (FTP)	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;

c) **All auditable events specified in ~~Table 3~~ 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 3~~ 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)
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
Unsuccessful attempt to validate a certificate	FIA_X509_EXT.1	Reason for failure of certificate validation

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 unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 **Refinement**: The TSF shall [“overwrite the oldest stored audit records”] and [*generate an email warning at 90%*] if the audit trail is full.

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.

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 cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1
- 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].

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.

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: [

- **RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2";**
- **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";**
- **Finite field-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 Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].**

] ~~**that meets the following: [assignment: list of standards]**~~.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_CKM.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];**

] 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, 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/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, 3072 bits*],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256 bits, 384 bits, 521 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, RFC 8017 (Section 8.2) [PKCS #1 v2.2], FIPS PUB 186-5 (Section 5.4) [RSASSA-PKCS1-v1_5].

Case: Elliptic Curve Digital Signature Algorithm schemes

- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D,
- Implementing “NIST curves” [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4

].

Application note: This SFR is modified by TD0999.

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 ~~cryptographic key sizes [assignment: cryptographic key sizes]~~ **message digest sizes [256, 384,512] bits** that meet the following: [**ISO/IEC 10118-3:2004**].

FCS_RBG_EXT.1 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 [CTR DRBG ([AES])].

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_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 [256, 384, 512] **and message digest sizes [256, 384, 512] bits** that meet the following: [**ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”**].

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 a specified cryptographic algorithm [

- AES used in [CBC, XTS] 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, and XTS as specified in IEEE 1619],

]

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] 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-256 (RFC 3602)] together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-256, HMAC-SHA-384].

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, RFCs 4109, [RFC 4304 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-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 time 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 time values can be configured within [*1-24*] hours;];].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (“x” in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*256*] bits.

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

- according to the security strength associated with the negotiated Diffie-Hellman group;
- 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 all IKE protocols implement DH Group(s) [

- [14 (2048-bit MODP)] according to RFC 3526,
- [19 (256-bit Random ECP), 20 (384-bit Random ECP)] according to RFC 5114.

].

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, ECDSA] 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: [SAN: IP address] and [no other reference identifier type].

FCS_KYC_EXT.1 Extended: Key Chaining

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [one, using a submask as the BEV or DEK] while maintaining an effective strength of [256 bits].

FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication

FCS_TLSC_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_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_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
- 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

] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6, IPv4 address in SAN].

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4 The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

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_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

] 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 [RSA with key size [2048 bits, 3072 bits], Diffie-Hellman parameters with size [2048 bits], ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves]].

FCS_TLSS_EXT.1.4 The TSF shall support [no session resumption or session tickets].

FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [4344, 5656, 6668].

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [no other method].

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*40,000*] bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr].

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha2-256, hmac-sha2-512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7 The TSF shall ensure that [ecdh-sha2-nistp256] and [ecdh-sha2-nistp384, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FCS_SSHC_EXT.1.9 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [no other methods] as described in RFC 4251 section 4.1.

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: [*Received faxes are automatically received and stored when receipt of faxes is enabled via device configuration. No U.ADMIN action is required per-fax. Only U.ADMIN with the Release Held Faxes permission may release held faxes for printing.*].

FDP_ACF.1.4 **Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*The Job Owner of submitted print jobs is determined by a Userid included in the embedded PJL. Print jobs received without a Userid, or with an unknown Userid, or with a Userid of a user that does not have the Held Jobs Access permission, are deleted after the specified timeout period for releasing held print jobs. During this time, no access to the print jobs is possible since access is restricted to the job owner*].

Table 18: D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
PRINT	**Operation:**	**Submit a document to be printed**	**View image or Release printed output**	**Modify stored document**	**Delete stored document**
	Job owner	(note 1) allowed	allowed	denied	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	(condition 1) allowed	denied	denied	denied
SCAN	**Operation:**	**Submit a document for scanning**	**View scanned image**	**Modify stored image**	**Delete stored image**
	Job owner	(note 2) allowed	denied	denied	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
COPY	**Operation:**	**Submit a document for copying**	**View scanned image or Release printed copy output**	**Modify stored image**	**Delete stored image**
	Job owner	(note 2) allowed	allowed	denied	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
FAX SEND	**Operation:**	**Submit a document to send as a fax**	**View scanned image**	**Modify stored image**	**Delete stored image**

		"Create"	"Read"	"Modify"	"Delete"
	Job owner	(note 2) allowed	denied	denied	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
FAX RECEIVE	**Operation:**	**Receive a fax and store it**	**View fax images or Release printed fax output**	**Modify image of received fax**	**Delete image of received fax**
	Fax owner	denied	denied	denied	denied
	U.ADMIN	denied	allowed	denied	allowed
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied

Table 19: D.USER.JOB Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
PRINT	**Operation:**	**Create print job**	**View print queue/job**	**Modify print job**	**Cancel print job**
	Job owner	(note 1) allowed	allowed	denied	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	allowed	denied	denied
	Unauthenticated	allowed	allowed	denied	denied
SCAN	**Operation:**	**Create scan job**	**View scan status/log**	**Modify scan job**	**Cancel scan job**
	Job owner	(note 2) allowed	allowed	denied	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	allowed	denied	denied

		"Create"	"Read"	"Modify"	"Delete"
	Unauthenticated	denied	allowed	denied	denied
COPY	**Operation:**	**Create copy job**	**View copy status/log**	**Modify copy job**	**Cancel copy job**
	Job owner	(note 2) allowed	allowed	denied	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	allowed	denied	denied
	Unauthenticated	denied	allowed	denied	denied
FAX SEND	**Operation:**	**Create fax send job**	**View fax job queue/log**	**Modify fax send job**	**Cancel fax send job**
	Job owner	(note 2) allowed	allowed	denied	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	allowed	denied	denied
	Unauthenticated	denied	allowed	denied	denied
FAX RECEIVE	**Operation:**	**Create fax receive job**	**View fax receive status/log**	**Modify fax receive job**	**Cancel fax receive job**
	Fax owner	denied	allowed	denied	denied
	U.ADMIN	denied	allowed	denied	allowed
	U.NORMAL	denied	allowed	denied	denied
	Unauthenticated	denied	allowed	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.

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_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.

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.

5.3.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to [

- *when a user attempts to login through EWS or the Control Panel*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [*lockout the user for an administrator configurable time period*].

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, role*].

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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [*other printable ISO 8859-15 set and Unicode/UTF-8 set characters except “>”*]];

- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 **Refinement:** The TSF shall allow [*job requests to be received via printing protocols*] 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 [*dots*] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

FIA_UID.1.1 **Refinement:** The TSF shall allow [*job requests to be received via printing protocols*] 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,* role*s*].

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: [

- *User's roles are associated with the user at initial authentication to the TOE.*

].

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: [*changes to a user role are effective at the next user login*].

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 [*lengths from 14 to 248 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] and be able to [use no other pre-shared keys].

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 [HTTPS, IPsec, TLS] 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 [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, [*State/Province Name, Locality Name, E-mail Address*]].

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 [*functions listed in Table 21*] 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 [change_default, query, modify, delete] the security attributes [*role and associated access permission]* 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	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	U.NORMAL (Authenticated user)
Authenticated user roles to copy, print, scan or fax on the TOE via EWS or the Control Panel.	Query	U.NORMAL (Authenticated user)

Data	Operation	Authorized role(s)
Authenticated user roles to copy, print, scan or fax on the TOE via EWS or the Control Panel.	Modify, Change default	U.ADMIN (System Administrator)
TSF Data not owned by a U.NORMAL		
Login password for System Administrator	Modify	U.ADMIN (System Administrator)
Software, firmware, and related configuration data		
Audit Log	Query, Modify behavior of	U.ADMIN
X.509 Certificate (TLS)	Modify, query, delete	U.ADMIN
IP filter table (rules)	Modify, query, delete	U.ADMIN
Email Addresses for fax forwarding	Modify, query, [*disable*]	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	Enable	Disable	Determine Behavior	Modify Behavior
Image Overwrite Security Enable/Disable, Scheduled	X	X	X	X
Enable/disable and configure smart card use	X	X	X	
Manage receive fax (job) passcodes			X	
Configure EWS and Control Panel session timeout	X	X	X	X
Configure users, roles, privileges and passwords	X	X	X	X
Configure network authentication	X	X	X	
Configure (specify the IP address and/or IP address range for remote trusted IT products (presumed) allowed	X	X	X	X

Management Functions	Enable	Disable	Determine Behavior	Modify Behavior
to connect to the TOE via the network interface) IP filtering				
Enable/disable and configure IPsec	X	X	X	X
Enable/disable and configure 802.1x	X	X	X	X
Create/upload/download X.509 certificates	X	X	X	
Enable/disable TLS	X	X	X	X
Transfer the audit records to a remote trusted IT product	X	X	X	
Configure SFTP	X	X	X	X
Enable/disable audit function	X	X	X	
Create a recurrence schedule for Image Overwrite	X	X	X	
Invoke Immediate Image Overwrite	X	X		
Invoke data purge function	X	X		
Enable/disable and configure fax forwarding to email	X	X	X	
Configure Software/Firmware updates	X	X		
Configure NTP	X	X	X	
Configure STARTTLS	X	X	X	

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] 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, digital signature data] 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 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 is modified by TD0927.

FPT_WIPE_EXT.1 Data Wiping

FPT_WIPE_EXT.1.1 The TSF shall ensure that any previous customer-supplied information content of a resource in non-volatile storage is made unavailable upon the request of an Administrator to the following objects: [**D.USER, D.TSF**] using the following method(s): cryptographic erase and [

- media specific eMMC method,

] that meets the following: [no standard].

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 [*time interval of user inactivity as follows:*

- *Control Panel will terminate any session that has been inactive for 1 minute;*
- *EWS will terminate any session that has been inactive for 60 minutes*].

5.3.8 Trusted Paths/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 **Refinement:** The TSF shall **use [IPsec, SSH, TLS, TLS/HTTPS] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: remote audit server, [authentication server, [*file server, mail server, NTP 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** [*user authentication, workflow scanning, scan to email*].

Application Note: Authentication server refers to both a KDC and a LDAP server (including Active Directory).

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 [IPsec, 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 actions**].

5.4 Assurance Requirements

37 The TOE security assurance requirements are summarized in Table 22.

Table 22: TOE Security Assurance Requirements

Assurance Class	Components	Description
Security Target (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

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

6.1 Identification and Authentication

6.1.1 I&A Methods (FIA_UAU.1 and FIA_UID.1)

39 The TOE provides the following means for users to identify and authenticate to the TOE:

a) **Local Authentication at EWS or Control Panel.** The TOE uses a local information database for users accessing through the Local UI (control panel) and EWS (browser based).

b) **Network Authentication at EWS or Control Panel.** The TOE uses LDAP to identify and authenticate users accessing through the Local UI and the EWS.

c) **Smartcard Authentication at the Control Panel.** Smart Card pin (only available for local access) validation of smartcard PKI credential is performed by a Windows Domain Controller in the TOE operational environment. The TOE uses Kerberos over IPsec to protect this communication.

40 The only operations permitted prior to successful identification and authentication are job requests received via printing protocols. The limited actions that are permitted before users are authenticated are noted in Table 18 and Table 19.

6.1.2 Lockouts & Timeouts (FIA_AFL.1 & FTA_SSL.3)

41 The TOE handles authentication failures as follows:

a) **EWS.** After five unsuccessful login attempts, where the login name or password were incorrect, the TOE shall impose a Lockout Period for that session only. The lockout period is configurable with the default being five minutes.

When the user's session is locked out for the EWS login, the user shall receive a message stating: "Your account is locked due to invalid login attempts. Please try again later.". This is to ensure that the user knows that the credentials were not necessarily wrong, but they were locked out and they should try later.

The Lockout Period time is initiated from the time of the fifth failed attempt. Further login attempts do not extend this period.

b) **Control Panel.** After five successive failed attempts to login at control panel (i.e. the user acknowledged the error and submitted incorrect data five times without canceling out of the authentication process) the device shall lockdown control panel Authentication.

The control panel shall continue to display the login prompt after the lockdown has been initiated.

All attempts to login at the control panel shall fail after the lockdown has been initiated, even if a valid username and password are provided.

The control panel lockdown shall last for minimum five minutes or more based on the time period configured by the administrator.

When the Control Panel or LUI is locked down after 5 unsuccessful authentication attempts, no user will be able to login at the LUI until the

configured lockout period has elapses, users other than the user that cause the lockout can login to EWS while the control panel is on lockout.

The control panel lockdown shall not impact a user's ability to access control panel pathways, services, and features that are accessible (not locked) to a non-logged-in user (unauthenticated). The lockdown shall only impact the things that require a user to authenticate.

42 By default, the control panel will terminate any session that has been inactive for 1 minute. By default, the EWS will terminate any session that has been inactive for 60 minutes. The system administrator can configure both the control panel and EWS session timeouts to terminate an inactive session after some other period of time.

6.1.3 Password Management (FIA_PMG_EXT.1 & FIA_UAU.7)

43 The valid character set for setting up passwords for accounts is the printable ISO 8859-15 set and Unicode/UTF-8 set, including: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", but not allowing the '>'character.

44 The maximum Password field length is limited by the device to a string of 63 octets (plus NULL1).

45 The System Administrator can set whether the password shall be required to contain at least one numeric character. The administrator can set the minimum required password length to be anywhere between 1 and 63 characters. When a user enters a password, only dots ("●") are displayed to obscure the password.

6.1.4 Authentication using X.509 certificates (FIA_X509_EXT.1, FIA_X509_EXT.2, and FIA_X509_EXT.3)

46 The TOE performs certificate validation in accordance with RFC 5280. Certificate validation occurs during HTTPS/TLS and IPsec connection establishment.

47 When certificates are used, the following certificate validation is performed:

a) The certificate path is validated, supporting a path length of 3.

b) The signature in each certificate in the path, using RSA (2048-bit or 3072-bit) or EC (256-bit, 384-bit, or 521-bit) digital signature algorithms, and is verified using the public key of the issuing CA certificate in the device's trust store.

c) The path must terminate with a CA certificate that has been configured as a trusted anchor.

d) All CA certificates in the path contain the basicConstraints extension with the CA flag set to TRUE.

48 Certificate revocation status is checked using OCSP as specified in RFC 6960. If an OCSP Responder cannot be contacted, the certificate is accepted. Revocation checking is performed for the entire certificate chain for certificates received from IPsec peers.

49 The TOE has a trust store where root CA can be stored. During certificate path validation, the TOE selects the appropriate trust anchor by matching the issuer of the presented certificate chain with a trusted CA certificate in the store. Only certificates that successfully chain to a configured trust anchor are accepted. Instructions for configuring the trusted IT entities to supply appropriate X.509 certificates are captured in the guidance documents.

50 In received certificates, for communications secured by IPsec, the SAN: IP Address must be present and is used as the presented identifier. For communications secured by TLS or HTTPS the IP address should present in CN or SAN to be used

as the presented identifier. The certificate of the OCSP Responder must contain the OCSP Signing purpose.

51 X.509 Certificate Signing Requests may be generated, containing 2 Letter Country Code, State/Province Name, Locality Name, Organization Name, Organization Unit, Common Name, and E-mail Address along with a generated 3072-bit RSA public key. Responses from a Certificate Authority are validated.

52 The TOE enforces the extendedKeyUsage field as follows:

- Server Authentication is required for certificates presented by remote TLS/HTTPS servers.
- OCSP Signing is required for certificates used by OCSP responders.

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

6.2 Auditing

6.2.1 Audit Events (FAU_GEN.1 & FAU_GEN.2)

54 The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to logged-in users, and each log entry contains a timestamp. The audit log also tracks user identification and authentication, administrator actions (including creation and modification of users and associated roles, as well as changes to the time), and failure of trusted channels.

55 Each log entry contains a time stamp, the type of event, the user that cause the event (where applicable), and the event outcome. For failure to establish a trusted communication channel, the log entry also contains the reason for the failure.

56 The TOE audit events are specified in Table 17. The TOE audit logs include a main audit log file and protocol log files.

6.2.2 Remote Audit Server (FAU_STG_EXT.1)

57 The TOE has the ability to transfer, or “push” the audit log file to a designated file server in the operational environment. This is possible via SFTP protocol only. The audit log transfer can be set up to send daily audit log file transmissions at a specific time, or a ‘send now’ function can be utilized to transfer audit logs immediately. Configuring the transfer or using the ‘send now’ feature is available via TOE EWS only.

6.2.3 Local Audit Store (FAU_STG.1, FAU_STG.4, FAU_SAR.1 and FAU_SAR.2)

58 Audit records are stored internally in the TOE and simultaneously transmitted to a configured remote syslog server over a secure SFTP/SSH trusted channel. The audit log may be accessed through the MFP via either the Embedded Web Server (EWS) or the Control Panel interface.

59 Only System Administrators with explicit Security Menu permission may view, download, or manage the local audit log. Regular users and administrators without this specific permission have no access to audit records under any circumstances. The audit log may be deleted by the System Administrator via the purge function described at section 6.10.1. Access control mechanisms preventing unauthorized access to the audit log are implemented as described in section 6.3.

60 The TOE can store a maximum of 15,000 audit log entries. The TOE overwrites oldest events first if the maximum is reached. When the TOE reaches 13,500 entries (90% full) an email warning is sent to a set of administrator defined email addresses. Subsequent warnings will be emailed after every 15,000 entries if the audit log has not been cleared.

6.2.4 Reliable Time (FPT_STM.1)

61 During initial device configuration the initial date and time are set. The TOE maintains the date and time to provide reliable timestamps. The TOE can also be configured to synchronize time with an NTP server in the operational environment.

6.3 Access Control

6.3.1 User Attributes & Roles (FIA_ATD.1, FIA_USB.1 and FMT_SMR.1)

62 The TOE maintains a username, role and password for each user. The role attribute defines the level of access that the user has to the TOE services and protected data. Upon successful authentication, the TOE associates the login user with the roles configured for that user. Users are granted access based on their role. Changes to user role are effective at the next user login.

63 The TOE ships with two pre-configured roles:

a) **System Administrator**. Has access to all pathways, services and features including all management functions on the TOE. This is the U.ADMIN role.

b) **Accounting Administrator**. Has access to all device services and pathways except for the tools pathway (which is used for System Administrator functions). This is a U.NORMAL role.

c) **Logged-in User**. Non-administrative users who have authenticated to the TOE. The System Administrator may create custom roles for Logged-In Users and assign MFD function privileges. This is a U.NORMAL role.

64 Upon successful authentication, users are granted access based on their role. Only a System Administrator is allowed access to all the TOE administration functions.

6.3.2 Control of Printer Functions (FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3)

65 Users (U.NORMAL) require explicit authorization from system administrators (U.ADMIN (System Administrator)) for them to be allowed to perform the following TOE Functions via the EWS or the Control Panel:

a) **Print**. Any host / authorized user on the network can submit print jobs, however, release of print jobs submitted by unknown/unauthenticated users to the hardcopy output handler is dependent on the system administrator defined policy.

b) **Scan**. Any host / authorized user on the network can submit Scan jobs.

c) **Fax**. Any host / authorized user on the network can submit LanFax jobs.

d) **Copy**. Any host / authorized user on the network can submit copy jobs.

66 During initial configuration of the TOE, the administrator must modify the access configuration for the different types of jobs at the local user interface. Initial values are permissive to unauthenticated users, and the administrator must set more restrictive settings to prevent access by unauthenticated users.

6.3.2.1 Print

67 Print jobs can be submitted remotely via printing protocols (e.g. lpr, port 9100) or from the EWS. Once submitted to the TOE, there is no way for anyone to modify the job (D.FUNC +PRT Modify) or the document (D.DOC +PRT Delete). None of the jobs will be processed until the job owner starts a user session at the local user interface. The authenticated job owner can release printing of the document (D.DOC +PRT Read) or delete the print job (D.FUNC +PTR Delete) at the local user interface. The owner may also choose to delete a job (submitted from the EWS) through the EWS before it is released.

68 Users have the option to assign a passcode to a print job during its submission (known as Secure Print). When required to enter the passcode, the user will need to be authenticated at the LUI in order to do so. The TOE can be configured to release Secure Print jobs with or without the associated passcode for the job owner who is authenticated at the LUI. User deletion of a Secure Print job requires knowledge of the associated passcode.

69 A system administrator has the capability to delete (D.FUNC +PRT Delete) print jobs at the LUI or EWS. The EWS only allows deletion of jobs submitted via the EWS.

6.3.2.2 Scan

70 Documents can only be scanned at the Local User Interface. During job setup, document image (D.DOC +SCN Read, Delete) may be read or deleted. Once the job is committed, the owner may send the image via email, transfer the image to a remote (TLS scan) repository, keep the image in their private mailbox or print the image.

71 (Scan to) Mailboxes are created and owned by individual users. Only the owner is allowed to locate and access the mailbox, and this access to mailboxes is further restricted with a passcode which the owner creates and owns. System Administrators have access to all the (scan) mailboxes. (Scan) Images saved in a mailbox (D.DOC +DSR and +SCN Read, Delete) may only be downloaded via the EWS or deleted. A user with proper access may choose to delete the mailbox together with all images stored inside the mailbox.

6.3.2.3 Fax

72 Faxes can be submitted at the Local User Interface or remotely as LanFax (through the same interfaces as for printing). During job setup, created document images may be read or deleted (D.DOC +faxOUT Read, Delete) by the job owner. Once a job is submitted, the job owner cannot delete the job itself, only a system administrator can delete the job before it is fully completed, in the case of delayed send for example (D.FUNC +faxOUT Delete). The job owner is permitted to delete stored images associated with their fax job prior to submission or during job setup.

73 Access to receive faxes is restricted to the system administrators (D.DOC +faxIN Read, Delete). All received faxes will be stored locally and assigned a system administrator predefined passcode. The system administrator can print or delete secure received faxes by entering the appropriate passcode. Once printed, the faxes are automatically deleted. Alternatively, the system administrator may also choose to designate email addresses for receiving fax images. Once the fax job is forwarded as an attachment to an email, the job is automatically deleted.

6.3.2.4 Copy

74 Copy has to be performed at the local user interface. A user can only read physical copies of the documents (D.USER.DOC +CPY Read). During job setup, the job owner may read or delete the image (D.DOC +CPY Read, Delete). A copy job

(D.USER.FUNC +CPY Delete, Modify) or image (D.DOC +CPY Read, Delete) can be read, modified or deleted. Once a job is committed, the job (D.FUNC +CPY Delete, Modify) can only be canceled (deleted) during its execution. Once completed, the job is removed

6.4 Administrative Roles

6.4.1 Secure Configuration (FMT_MOF.1, FMT_SMF.1, FMT_MTD.1)

75 All management functions are only usable by the System Administrator. The System Administrator specifies whether management functions can be enabled, disabled, and determines or modifies the behavior of the function. See Table 21 for specific management functions, these functions can be performed via the EWS or the Control Panel.

76 As previously described, the TOE enforces a System Administrator defined role-based access control policy. Table 20 specifies the management of TSF data and what each role is permitted to do for TSF data.

6.5 Trusted Operation

6.5.1 Secure Boot (FPT_SBT_EXT.1)

77 During initial start-up, the TOE performs self-tests on the cryptographic components. The following tests are performed during start-up:

- Executable code integrity testing – A digital signature (RSA-2048 with SHA-256) protecting boot firmware components is verified using the embedded public verification key.
- Cryptographic algorithm testing – Uses Known Answer Tests (KATs) to verify proper operation of cryptographic functions.

78 During the boot cycle, the integrity of the executable code is validated. During manufacturing, write-once fuses are programmed with a SHA-256 hash of Lexmark's public code signing key. This hash is immutable and cannot be modified after manufacturing. The boot ROM verification logic itself resides in immutable on-chip ROM and cannot be modified post-manufacturing. The boot ROM will refuse to load any code that is not signed by the key whose hash does not match that which was programmed at manufacturing.

79 The Hardware Root of Trust contains an immutable SHA-256 hash of the vendor public signing key and the boot ROM verification logic, which serves as the anchor for the verification chain. The Root of Trust does not store private keys. This data verifies the authenticity of the public key presented during boot, which in turn verifies the signatures of boot components.

80 At power on, the boot ROM looks for an image description table on the designated boot device. The image description table contains the size, location, and hash of the next stage boot loader (g2-loader), the hash of the u-boot image, and a public key. The image description table is signed, and the boot ROM verifies the signature using the provided public key. The boot ROM also verifies that the SHA-256 hash of the public key matches the hash programmed in the hardware fuses. The boot ROM loads g2-loader into SRAM, verifies its SHA-256 hash, and control is passed to g2-loader only if both the digital signature verification and hash verification succeed.

81 g2-loader initializes DRAM and some other platform-specific pieces before loading the next stage boot loader, u-boot. g2-loader uses the same image description table for loading and verifying u-boot, and verifies the SHA-256 hash of u-boot against the

reference hash contained in the previously verified image description table. Control is passed to u-boot only if the hash verification succeeds. Because the image description table was digitally signed and validated in Stage 1, the integrity of u-boot remains cryptographically anchored in the Hardware Root of Trust.

82 u-boot then looks for a kernel (and optionally initramfs) to load. The entire cramfs partition is loaded into memory. At the end of the partition is a certificate with signature. u-boot verifies the signature of the entire partition, and verifies that the signature was made by the same key that is baked into u-boot (the public side of the key is hard-coded in u-boot source code). The digital signature covers the entire boot partition, including the Linux kernel and the dm-verity root hash metadata. Control is passed on to the kernel in the boot partition.

83 The boot partition also contains information that is used by the dm-verity subsystem of the Linux kernel. This information is covered by the same signature as the rest of the boot partition. The kernel uses this information to create a dm-verity device, which the kernel then mounts for the root filesystem. The dm-verity subsystem validates each data block hash and intermediate Merkle tree hash up to the root hash verified in the previous stage. Since changing any part of the root filesystem would invalidate the verity hashes, a read-only filesystem is required, for which Lexmark uses squashfs.

84 If code verification fails, including any digital signature verification or hash validation failure at any stage of the secure boot chain, all the imaging and mechanism control blocks of the HCD, as well as network and PCIe functionality, is disabled and the system halts. The only way to proceed is to reboot the HCD. The TOE enters a secure boot failure state and displays an error condition indicating that vendor support should be contacted.

85 Xerox trusted boot verification now authenticates the non-root file system boot objects up to and including the Trellix security modules. Integrity validation is performed using a hash table of boot components and a separate hash table of Trellix components, each protected by a digital signature. The TOE verifies the signature of each hash table and validates the SHA-256 hash of each listed component prior to execution. Components that fail verification are not executed

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

6.5.2 Self-tests (FPT_TST_EXT.1)

87 The TOE preforms the follow start-up self-tests:

a) **Secure Boot**. As described in section 6.5.1, the TOE implements a chain of trust with digital signature verification at each stage of the boot process.

b) **Cryptographic Module Verification.** The Mocana cryptographic modules, which are FIPS 140-3 compliant, performs self-tests upon initialization. These tests include HMAC-SHA-256 software integrity testing that verifies the integrity of the modules by executing the HMAC-SHA 256 fingerprint algorithm on the shared library .so file, and comparing the result with the signature file. If any test fails, the system halts operation of the affected module. This integrity check is performed as part of the function FIPS_powerupSelfTest(). This function is called automatically by the host O/S upon loading the shared object into memory.

88 Together, the above tests are sufficient to demonstrate that the TSF is operating correctly by verifying the TSF’s code integrity along with verifying the correct operation of the cryptographic module.

6.5.3 Trusted Update (FPT_TUD_EXT.1)

89 The System Administrator may view the current version of TOE firmware via EWS or the Control Panel and may initiate updates to TOE firmware via EWS.

90 Firmware update images are digitally signed (RSA2048 / SHA-256). The TOE verifies the digital signature prior to installing the update. A failure will result in the update being aborted.

6.6 Cryptographic Operations

6.6.1 Key Management (FCS_CKM.1/AKG, FCS_CKM.1/SKG, FCS_CKM.2, FCS_CKM.4, FCS_CKM_EXT.4, FCS_RBG_EXT.1, FPT_SKP_EXT.1)

91 The TOE cryptographic module implements random bit generation services using CTR_DRBG (AES), which is invoked during key generation operations, and is seeded with a minimum of 256-bits of entropy from a hardware noise source as further described in the separate proprietary Entropy Description document.

92 The TOE generates cryptographic keys at initial start-up when an administrator generates a new key pair, when users change their passwords, and during secure channel communications.

93 The TOE generates the following cryptographic keys:

a) FFC with key sizes of 2048-bit or greater

b) FFC using “safe-prime” DH Group 14 (2048-bit MODP), Group 19 (256-bit Random ECP), Group 20 (384-bit Random ECP) per NIST SP 800-56A Rev 3 “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526.

c) RSA 2048 and 3072 per FIPS PUB 186-4 “Digital Signature Standard (DSS)” Appendix B.3.

d) ECC schemes using NIST curves P-256, P-384, and P-521 per FIPS PUB 186-4 “Digital Signature Standard (DSS)” Appendix B.4

e) 128-bit and 256-bit symmetric keys that meet NIST SP 800-133 Rev.2 Section 6.1, which are obtained directly from the CTR_DRBG as specified in FCS_RBG_EXT.1.

94 The TOE supports the following asymmetric key establishment schemes. Each scheme is mapped to its corresponding SFR and service and complies with the referenced standards.

Table 23: Cryptographic Scheme Mapping

Scheme	SFR	Service/Usage
RSA	FCS_TLSS_EXT.1	EWS server
	FCS_TLSC_EXT.1	Repository file server LDAP server Mail server

Scheme	SFR	Service/Usage
	FCS_IPSEC_EXT.1	Print and fax job transmission Smartcard authentication
ECC	FCS_TLSS_EXT.1	EWS server
	FCS_TLSC_EXT.1	Repository file server LDAP server Mail server
	FCS_IPSEC_EXT.1	Print and fax job transmission Smartcard authentication
	FCS_SSHC_EXT.1	Log file transfer to remote server
FFC	FCS_TLSS_EXT.1	EWS server
	FCS_TLSC_EXT.1	Repository file server LDAP server Mail server
FFC using “safe-prime”	FCS_IPSEC_EXT.1	Print and fax job transmission Smartcard authentication

95 **Note**: The FFC scheme uses safe-prime parameters as defined in RFC 3526 Section 3.

96 Keys and keying material are securely deleted when no longer needed. Keys in volatile memory are destroyed by removal of power to the memory. For keys in non volatile memory, the TOE destroys them by logically overwriting the previous keys with newly created keys of the same size. Table 24 below lists when key and key material are no longer needed.

97 Key generation and destruction are further described in a separate proprietary Key Management Document. There are no known configurations or circumstances that do not conform to the key destruction requirement.

98 All private, pre-shared and symmetric keys are stored on encrypted partitions of the internal eMMC, which is the TOE’s only non-volatile storage device. All eMMC partitions containing TOE data are encrypted; no plaintext or non-encrypted partitions exists in the evaluated configuration. The TOE uses AES-CBC-256 for all data encryption. See Table 24 for specific keys and their corresponding storage resource.

99 The TOE does not allow users or the System Administrator, through any customer provided interface, to view or obtain any pre-shared key, private key, or symmetric key.

Table 24: Keys and CSPs

Key/CSP	Type / Strength	Storage	Protection	End-of-life / When key is destroyed
BEV	256-bit symmetric	Refer to KMD for details.		
DEK	256-bit symmetric			
IKE Device Certificate Private Key	RSA-2048 ECDSA-P256/P384 /P521	Encrypted File System	AES-CBC-256	When a certificate is deleted by the TOE administrator.
		RAM	n/a	Destroyed at power off.
IKE Pre Shared Key	UTF-8 encoding of passphrase Minimum 14 bytes	Encrypted File System	AES-CBC-256	When a new pre-shared key is configured.
		RAM	n/a	Destroyed at power off.
IKE session authentication key	HMAC-SHA-256/384	RAM	n/a	Destroyed at power off.
IKE session encryption key	AES-CBC-128/256	RAM	n/a	Destroyed at power off.
IPSec session encryption key	AES-CBC-128/256	RAM	n/a	Destroyed at power off.
IPSec session authentication key	HMAC-SHA-256/384	RAM	n/a	Destroyed at power off.
SSH Private Key	RSA-2048 ECDSA-P256/P384/P521	Encrypted File System	AES-CBC-256	When generating a new keypair.
		RAM	n/a	Destroyed at power off.
SSH Session Authentication Key	HMAC-SHA-256/512	RAM	n/a	Destroyed at power off.
SSH Session Encryption Key	AES-128/256	RAM	n/a	Destroyed at power off.
SSH Key Exchange Key	ECDH-P256/P384/P521	RAM	n/a	Destroyed at power off.

Key/CSP	Type / Strength	Storage	Protection	End-of-life / When key is destroyed
TLS Server Private Key	RSA-2048 ECDSA-P256/P384 /P521	Encrypted File System	AES-CBC-256	When a certificate is deleted by the TOE administrator.
TLS Session Authentication Key	HMAC-SHA2-256/384	RAM	n/a	Destroyed at power off.
TLS Session Encryption Key	AES-128/256	RAM	n/a	Destroyed at power off.
User Passwords (Local Authentication)	Configurable by Admin to a minimum of 15 bytes	Encrypted File System	AES-CBC-256	When a user changes their password. When a user is deleted.

6.6.2 Encryption/Decryption (FCS_COP.1/DataEncryption, FCS_COP.1/StorageEncryption)

100 The TOE supports the following (algorithm-mode-key sizes):

- AES-CBC-128/256 for TLS, IPsec and SSH
- AES-GCM-128/256 for TLS
- AES-CBC/XTS-256 for disk encryption

6.6.3 Signature Generation/Verification (FCS_COP.1/SigGen)

101 The TOE supports the following digital signature generation and verification services:

- RSA 2048, 3072 (FIPS 186-4)
- ECDSA P-256, P-384, P-521 (FIPS 186-4)

6.6.4 Hashing Services (FCS_COP.1/Hash, FCS_COP.1/KeyedHash)

102 The TOE provides cryptographic hashing services using SHA2-256, SHA2-384, and SHA2-512. SHA is used in: TLS, IPsec, SSH, Trusted Update (digital signature verification), and Storage Encryption.

103 The TOE implements HMACs as shown Table 25. HMAC is used in: TLS, IPsec, and SSH.

Table 25: HMAC Characteristics

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA2-256	512 bits	256 bits	256 bits
HMAC-SHA2-384	1024 bits	384 bits	384 bits
HMAC-SHA2-512	1024 bits	512 bits	512 bits

6.6.5 Cryptographic Algorithm Validation Certificates

104 Table 5 provides a mapping between the SFRs and CAVP certificates. The TOE incorporates the following cryptographic module:

- **Mocana Cryptographic Library v7.0.0f_u1**. SSH, TLS, IKE, and Disk encryption.
- **Mocana Cryptographic Library 7.0.0f**. IPsec, and Disk encryption.

6.7 Data Encryption

6.7.1 Drive Encryption (FDP_DSK_EXT.1)

105 The TOE implements full drive encryption that is enabled by default as shipped from the factory and is performed in accordance with FCS_COP.1/StorageEncryption**.**

106 All user document data and confidential TSF data, including all temporary files created during a copy, print, scan, or fax job, are stored in an encrypted state. All partitions of the drive used for spooling temporary files are encrypted.

107 The TOE makes use of block-level software encryption and the Mocana cryptographic library to perform transparent disk encryption.

108 Proprietary details on the disk encryption implementation and unencrypted/encrypted partitions are provided in the KMD.

6.7.2 Key Chain (FPT_KYP_EXT.1 & FCS_KYC_EXT.1)

109 The TOE generates a 256-bit BEV for disk encryption. The BEV is stored in the TPM and retrieved from the TPM during boot. A SHA2-256 hash of the BEV is used as the DEK. Further details are provided in the KMD.

6.8 Trusted Communication

6.8.1 Communication Paths (FTP_ITC.1, FTP_TRP.1/Admin, FTP_TRP.1/NonAdmin)

110 Section 2.2.3 identifies the communication paths and related protocols used by the TOE. The following sections provide protocol-specific details.

6.8.2 HTTPS (FCS_HTTPS_EXT.1)

111 The TOE's EWS interface is accessed via HTTPS, in this case the TOE is a HTTPS/TLS server. TOE users, access EWS via a web browser and authenticate as described section 6.1. TLS client authentication is not supported.

112 The TOE is also capable of sending scanned images over HTTPS to a Workflow Repository file server. In this case, the TOE is a HTTPS/TLS client. TLS client authentication is not supported.

113 HTTPS is implemented in the TOE according to RFC 2818, which specifies HTTP over TLS.

114 Furthermore, as mentioned in section 6.8.3, the TOE verifies the identity of the HTTPS server using the DNS name or IP address presented in the Subject Alternative Name (SAN) field of the server certificate. The TOE compares the presented identifier with the configured reference identifier and terminates the connection if they do not match. The TOE supports DNS-name wildcard matching. Certificate validation failures result in the connection being rejected. After successful

handshake, all HTTP data transmit as TLS application data as per section 2.1 of RFC 2818.

6.8.3 TLS (FCS_TLSC_EXT.1 & FCS_TLSS_EXT.1)

115 The TOE implements a TLS server in support of the EWS interface (HTTPS). The TOE implements a TLS client in support of communication with the LDAP server (LDAPS), Mail Server (STARTTLS) and Workflow Repository File Server (HTTPS).

116 The TLS server and client implementation supports TLS 1.2 and the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

117 TLS client authentication is not supported.

118 The TLS client implementation verifies server certificates according to RFC 6125 section 6 and IPv4 addresses in the Subject Alternative Name (SAN) extension. The TOE supports reference identifiers in the form of DNS names per RFC 6125 section 6, and IPv4 addresses which appear in the Subject Alternative Name (SAN) extension of the server certificate. When an IPv4 address is used as a reference identifier, the TOE converts the textual representation to a binary representation in network byte order following the canonical format specified in RFC 3986. Wildcards are supported by the TLS client interface.

119 The reference identifiers are configured by an administrator in the remote server configuration interfaces (for LDAP server, Mail Server, and Workflow Repository File Server). During the TLS handshake, the TOE compares the reference identifier against the presented identifier in the server certificate. If the identifiers do not match, the TLS connection is not established. The TOE does not implement any administrator override mechanism for certificate validation failures.

120 When initiating a TLS connection, the client presents the Supported Elliptic Curves/Supported Groups Extension in the Client Hello message with the following curves: secp256r1, secp384r1, and secp521r1. This behavior is performed by

default and cannot be modified through configuration. These elliptic curves support the ECDHE key establishment schemes used in the supported cipher suites.

121 The TOE's TLS server implementation explicitly denies connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1. When a client attempts to establish a connection using these older protocols, the TOE actively rejects the connection attempt by sending an appropriate alert message and terminating the handshake. This ensures that only TLS 1.2 connections are established, as specified in the supported protocol versions.

122 For key establishment in TLS server mode, the TOE uses:

- RSA with 2048-bit or 3072-bit keys
- ECDHE with the elliptic curves secp256r1, secp384r1, and secp521r1
- DHE using 2048-bit parameters

123 These same key establishment methods and parameters are supported in TLS client mode.

124 The TOE's TLS server implementation does not support session resumption or session tickets.

6.8.4 SSH Client (FCS_SSHC_EXT.1)

125 The TOE implements the SSH/SFTP protocol for transferring audit records to a remote audit server, in accordance with RFCs 4251, 4252, 4253, 4254, 4344, 5656, and 6668, supporting the public key-based authentication as specified in RFC 4252 and no other methods of authentication.

126 For public key-based authentication, the TOE supports the following public key algorithms:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384

127 The TOE client can authenticate itself to a remote SSH server by using a locally stored private key corresponding to one of the supported public key algorithms. The authentication process follows RFC 4252 Section 7, where the client signs a message using its private key to prove identity to the server.

128 In accordance with RFC 4253, the TOE monitors the size of packets received on an SSH transport connection. Any packet exceeding 40,000 bytes is automatically dropped by the SSH client implementation.

129 The TOE's SSH client implementation supports the following encryption algorithms as specified in RFC 4253: aes128-cbc, aes256-cbc, aes128-ctr, or aes256-ctr.

130 Supported public key algorithms for authenticating remote audit servers are ecdsa-sha2-nistp256, and ecdsa-sha2-nistp384.

131 Supported data integrity MAC algorithms are hmac-sha2-256, or hmac-sha2-512.

132 The TOE supported key exchange methods are ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521.

133 The TOE maintains a local database that associates each remote audit server’s hostname with its corresponding public key. During connection establishment, the TOE verifies the server’s identity by matching the presented public key against the stored key for the given hostname, in accordance with RFC 4251 Section 4.1.

134 By default, the thresholds described in FCS_SSHC_EXT.1.8 are not reached due to limitation by the TOE. Due to the short period in which this channel remains open to perform the transmission of audit data to an external IT entity, and the nature of this traffic being minimal in size, the transmission occurs rapidly and therefore will not trigger the time-based or traffic-based thresholds addressed by the SFR.

135 The TOE does not receive files over SFTP. No other SSH protocol characteristics are supported.

6.8.5 IPsec (FCS_IPSEC_EXT.1, FIA_PSK_EXT.1)

136 The TOE uses IPsec for communication with a Domain Controller for Smart Card authentication and to protect communication with all remote print clients. Additionally, to secure time synchronization with NTP servers the TOE implements IPsec.

137 The TOE implements an IPsec Security Policy Database (SPD) and allows configuration to discard, bypass, and protect packets.

138 Policies are configured at the TOE EWS configuration pages. In the configuration, Policies consist of combinations of three parts: Host Group, Protocol Group, and Actions (bypass, discard, protect). Several policies can be configured and are listed in order on the EWS in the IPsec configuration page. The SPD which consists of these policies is consulted during the processing of all traffic, both inbound and outbound. The entries in the SPD are ordered as displayed on the policy list on the EWS. A match is made when the host/host group, and protocol/protocol group in the SPD policy matches these values in an incoming or outgoing packet. As a packet is analyzed, the policies are consulted in order and the first matched policy will be used to process the traffic, and the associated action applied.

139 For the evaluated configuration, only inbound connections are supported for reception and handling of print jobs; outbound connections for transmission of scan jobs are not supported. A final policy is configured such that any non-matching packet results in the packet being discarded. These IPsec policies, set up via the EWS IPsec configuration page, correspond to the evaluated configuration.

140 Components of Policies (host/host group, protocol/protocol group, action):

a) Host/Host Group: A host group is a non-empty set of addresses over which to apply the policy. Three types of hosts can be set: Any, a subnet, or a specific address. Subnet and individual settings may be simultaneously set.

b) Protocol/Protocol Group: The Protocol Groups section defines the upper layer protocols that are to be part of the defined policy. Valid choices include All, FTP, HTTP, SMTP, IPP, and others that can be selected from a list at the EWS, or manually entered as TCP/UDP and port number.

c) Action: Action of Protect: The following cryptographic protocols are supported:

   i) Authentication Header (AH)-Allows authentication of the sender of data.

   ii) Encapsulating Security Payload (ESP)-Supports both sender authentication and data encryption.

141 Both transport and tunnel mode are supported and are configuration options when configuring up IPsec.

142 The IPsec ESP protocol is implemented in conjunction with AES-CBC-128 and AES-CBC-256 together with the following SHA-based HMAC algorithms: HMAC-SHA2-256 and HMAC-SHA2-384.

143 IKEv1 is implemented with main mode only for phase 1 key exchanges. Aggressive mode is not supported. AES-CBC-128 or AES-CBC-256 may be used for encrypting the IKEv1 payload.

144 IKEv1 Phase 1 associated key lifetime can be configured in seconds, minutes, or hours, with the maximums being 86400, 1440, and 24 respectively. DH Group 14(2048-bit MODP), DH Group 19 (256-bit Random ECP), and DH Group 20 (384 bit Random ECP) are the only DH groups allowed.

145 IKEv1 Phase 2 associated key lifetime can be configured in seconds, minutes, or hours, with the maximum values being 28800, 480, and 8 respectively. Phase 2 negotiations use the security associations established during Phase 1 and can employ DH group 14 (2048-bit MODP), DH Group 19 (256-bit Random ECP), DH Group 20 (384-bit Random ECP) for Perfect Forward Secrecy (PFS).

146 The TOE can be configured to perform peer authentication in IKE Phase 1 using either RSA/ECDSA certificates or pre-shared keys. If the TOE is configured to use certificates, the TOE will perform peer authentication using a device authentication certificate and a server validation certificate. The administrator can configure the TOE to use either digital certificates (RSA or ECDSA) or pre-shared keys for Phase 1 peer authentication by creating an IP policy rule in the TOE's IP Security Policy.

147 The TOE verifies the peer’s identity during IKE Phase 1 by comparing the Subject Alternative Name (SAN) field in the peer’s certificate against the configured reference IP address. Only the SAN:IP value is used for this comparison; the Common Name (CN) and other fields are ignored. The TOE establishes a trusted IPsec channel only if the SAN:IP exactly matches the configured reference identifier; otherwise, the connection is rejected.

148 The pre-shared key is configurable with an ASCII text string with range of 14 – 248 characters. This includes the construction of the 22 octet length pre-shared key. The pre-shared key is initially conditioned using a SHA-256 hash and then encrypted with AES 256 algorithm, and securely destroyed with overwrites on deletion or replacement.

149 The TOE generates the Diffie–Hellman private value x using the CTR_DRBG (AES-256) 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
- Group 19 (256-bit Random ECP) according to RFC 5114
- Group 20 (384-bit Random ECP) according to RFC 5114

150 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.

151 The TOE also generates nonces used in IKEv1 exchanges using the random bit generator specified in FCS_RBG_EXT.1. All nonces are generated according to the security strength associated with the negotiated Diffie-Hellman group. All nonces generated are at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash.

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

153 The pre-shared key is configurable with an ASCII text string with range of 14 – 248 characters. This includes the construction of the 22 octet length pre-shared key. The

pre-shared key is initially conditioned using a SHA-256 hash and then encrypted with AES 256 algorithm, and securely destroyed with overwrites on deletion or replacement.

6.9 PSTN Fax-Network Separation

6.9.1 Separation (FDP_FXS_EXT.1)

154 The only communication via the fax interface allowed is that of transmitting or receiving User Data using the T.30 fax transmission protocol.

155 The TOE provides separation between the fax processing board and the network interface and therefore prevents an interconnection between the PSTN and the internal network. This separation is realized in software, as by design, these interfaces may only communicate via an intermediary. All internal command calls (API) and response messages for both the network and fax interfaces are statically defined within the TOE. No user or System Administrator is able to change their formats or functionalities.

156 The fax software runs two independent processes, for sending and receiving job data through the fax card respectively. There is no internal communication between these two processes.

157 The same job data will never be active on both the fax interface and network interface at the same time. For network interface to fax interface (LanFax) jobs, the entire job must be received as an image and buffered in memory before it is sent out through the fax interface. Likewise, for fax interface to network interface (fax forwarding to email) jobs, the entire job must be received from the fax interface and buffered in memory before it is transformed by an intermediary subsystem into an email attachment and sent out through the network interface.

6.10 Data Clearing and Purging

6.10.1 Wipe Data (FPT_WIPE_EXT.1)

158 The purge function is invoked manually by the system administrator through the control panel. The function securely wipes all customer-supplied data (D.USER) and TSF data (D.TSF) stored in non-volatile storage locations, including:

- **User documents.** All active and queued jobs on eMMC
- **User function data**. Job history and log files on the eMMC
- **User authentication data**. Local credentials in the internal database
- **User address data**. Address books and contact information
- **TSF data**. Configuration settings and accounting databases

159 The purge process employs a media-specific eMMC method, relying on Trim and Garbage Collection mechanisms provided by the eMMC controller. These operations instruct the controller to mark blocks containing sensitive data as invalid and allow the internal wear-leveling and garbage collection algorithms to reclaim and overwrite them. This approach is designed to make previously stored data inaccessible, even on wear-leveled flash media.

7 Rationale

7.1 Conformance Claim Rationale

160 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

161 The Security Objectives are reproduced from the HCDcPP.

7.3 Security Assurance Requirements rationale

162 The Security Assurance Requirements are as defined by the HCDcPP.