Xerox® AltaLink™ EC8036 & EC8056

Security Target

Version 1.4

June 2022

Document History

Version	Date	Description
1.0	7 Jan 2022	Release for certification.
1.1	15 Mar 2022	Update TOE version.
1.2	14 Apr 2022	Section 5.3.2 update.
1.3	19 May 2022	Addressed OR16
1.4	1 June 2022	Addressed OR18

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Xerox® AltaLink™ EC8036 & EC8056 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE is a network copier and printer with scan and fax capabilities.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Xerox® AltaLink™ EC8036 & EC8056 Software Version: 103.023.031.35105
Security Target	Xerox® AltaLink™ EC8036 & EC8056 Security Target, v1.4

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) Protection Profile for Hardcopy Devices, v1.0

e) Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

f) NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name
TD0074	FCS_CKM.1(a) Requirement in HCD PP v1.0
TD0157	FCS_IPSEC_EXT.1.1 – Testing SPDs
TD0176	FDP_DSK_EXT.1.2 – SED Testing
TD0219	NIAP Endorsement of Errata for HCD PP v1.0
TD0253	Assurance Activities for Key Transport
TD0261	Destruction of CSPs in flash
TD0299	Update to FCS_CKM.4 Assurance Activities
TD0393	Require FTP_TRP.1(b) only for printing
TD0474	Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1

TD #	Name
TD0494	Removal of Mandatory SSH Ciphersuite for HCD
TD0562	Test activity for Public Key Algorithms

1.4 Terminology

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

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
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
HDD	Hard Disk Drive
I&A	Identification and Authentication
KMD	Key Management Description (Xerox proprietary)
LanFax	Enables fax jobs to be submitted from the desktop via printing protocols.
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

Term	Definition
SMTPS	Simple Mail Transfer Protocol Secure
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

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.

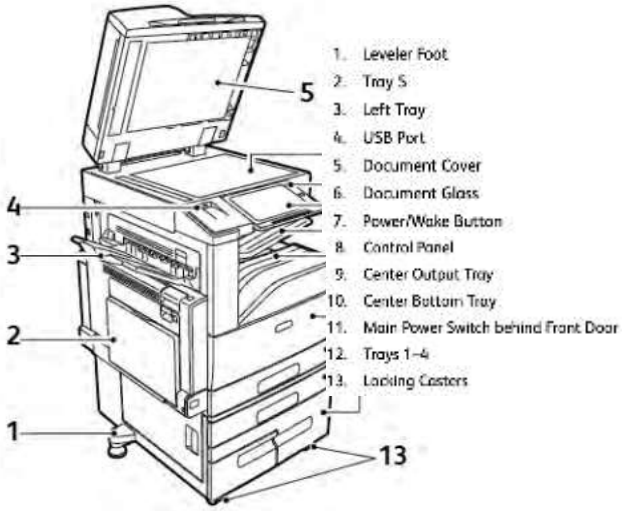

Figure 1: TOE Front View

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 (see Figure 1 item 8), which provides status information, allows device configuration and provides access to hardcopy functions.

7 In addition to the Control Panel, user 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 hardcopies 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 2.4.2). 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 SMTPS**.**

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 2.4.2). 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 SMTPS.

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.

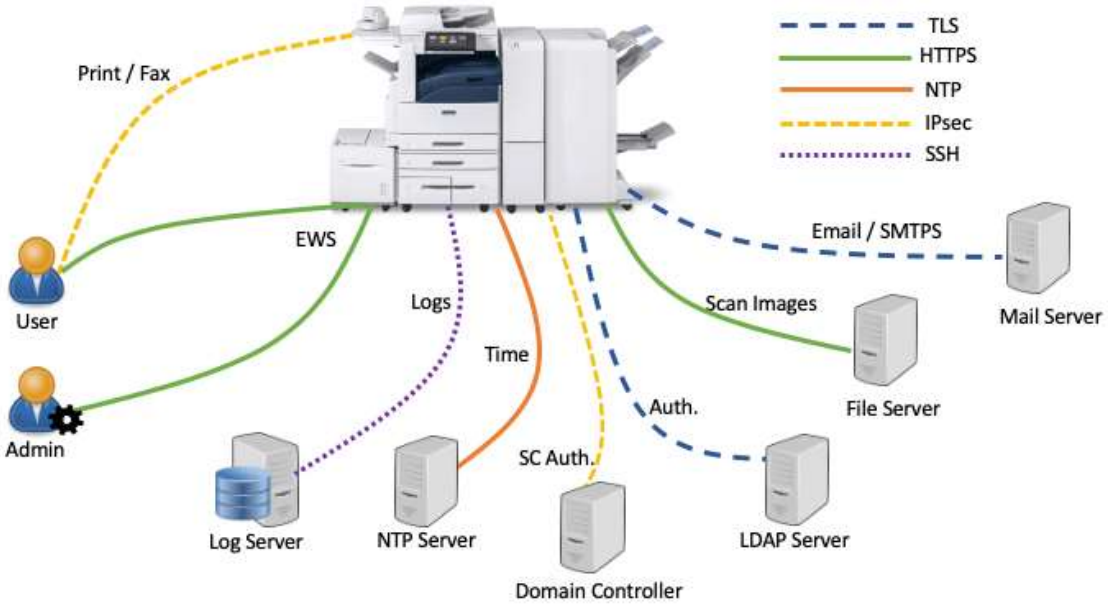

Figure 2: TOE Secure Communication

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) **Security Audit.** 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.

c) **Access Control.** The TOE enforces a system administrator defined role-based access control policy.

d) **Security Management.** System administrators mange the TOE's security configuration via the Control Panel and/or EWS. The TOE allows filtering rules to be specified for IPv4 network connections based on IP address and port number.

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

f) **Cryptographic Operations.** The TOE incorporates two cryptographic modules:

   i) **Mocana.** Provides cryptographic services for hard disk encryption/decryption and encryption/decryption services for the IPSec protocol and for asymmetric key generation

   ii) **OpenSSL.** Provides cryptographic services for HTTPS/TLS and SSH encryption/decryption services.

g) **Storage Encryption.** The TOE stores temporary files created during a copy, print, scan and fax job on a single shared hard disk drive (HDD). All partitions of the HDD used for spooling temporary files are encrypted.

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

i) **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.

j) **Data Clearing and Purging.** The image overwrite feature overwrites temporary image files created during a copy, print, scan or fax job when those files are no longer needed. Overwrite is also invoked at the instruction of a job owner or administrator and at start-up. 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.

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.

Table 4: TOE models

Model	Firmware Version	CPU / OS
AltaLink™ EC8036	103.023.001.05400	Intel Atom E3845 (Bay Trail) Wind River Linux 6.0 (Linux 3.10 32-bit)
AltaLink™ EC8056		

2.4.1 Guidance Documents

14 The TOE includes the following guidance documents (PDF):

a) Secure Installation and Operation of your Xerox® AltaLink® EC8036/EC8056 Color Multifunction Printer, v1.1, December 2, 2021

b) Xerox® EC8036/EC8056 Color Multifunction Printer System Administrator Guide, v1.0, July 2021 (702P08632)

c) Xerox® EC8036/EC8056 Color Multifunction Printer User Guide, v1.0, July 2021 (702P08641)

d) Xerox® EC8036/EC8056 Color Multifunction Printer Getting Started Guide

e) Xerox® AltaLink® Series Smart Card Installation and Configuration Guide, v3.0, December 2020 (702P08579)

2.4.2 Non-TOE Components

15 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/product/xerox-ec8036-ec8056-multifunction-printer/downloads?platform=win10x64&language=en

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

16 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) Internet Fax

f) Embedded Fax mailboxes

g) Wi-Fi Direct Printing

h) Weblet Services

i) InBox Apps

j) Remote Control Panel
k) SFTP when used for scanning
l) SNMPv3
m) Scan to USB
n) Print from USB
o) SMB Filing
p) Convenience Authentication
q) Xerox Workplace Cloud
r) Proximity Card Authentication

3 Security Problem Definition

17 The Security Problem Definition is reproduced from section 2 of the HCDPP.

3.1 Threats

Table 5: Threats

Identifier	Description
T.UNAUTHORIZED_ ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_ COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate while in a degraded state.
T.UNAUTHORIZED_ UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_ COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.2 Assumptions

Table 6: 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.

3.3 Organizational Security Policies

Table 7: 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 protected and transmitted to an External IT Entity.
P.COMMS_ PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_ OVERWRITE	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.
P.PURGE_DATA	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.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 8: 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.

Identifier	Description
O.USER_ AUTHORIZATION	The TOE shall perform authorization of Users in accordance with security policies.
O.ADMIN_ROLES	The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.
O.UPDATE_ VERIFICATION	The TOE shall provide mechanisms to verify the authenticity of 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 be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the TOE.
O.STORAGE_ ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data in Field-Replaceable 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 Field-Replaceable 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	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.IMAGE_ OVERWRITE	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.
O.PURGE_DATA	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.

4.2 Security Objectives for the Operational Environment

Table 9: 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

18 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").

19 **Note:** Operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the HCDPP.

5.2 Extended Components Definition

20 Refer to HCDPP for extended component definitions.

21 Extended components are identified by "EXT" appended to the SFR identifier.

5.3 Functional Requirements

Table 10: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.4	Prevention of Audit Data Loss
FCS_CKM.1(a)	Cryptographic Key Generation (for asymmetric keys)
FCS_CKM.1(b)	Cryptographic Key Generation (for Symmetric keys)
FCS_CKM_EXT.4	Extended: Cryptographic Key Material Destruction
FCS_CKM.4(a)	Cryptographic Key Destruction
FCS_COP.1(a)	Cryptographic Operation (Symmetric Encryption/Decryption)
FCS_COP.1(b)	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1(c)	Cryptographic operation (Hash Algorithm)

Requirement	Title
FCS_COP.1(d)	Cryptographic operation (AES Data Encryption/Decryption)
FCS_COP.1(g)	Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
FCS_IPSEC_EXT.1	Extended: IPsec selected
FCS_HTTPS_EXT.1	Extended: HTTPS selected
FCS_KYC_EXT.1	Extended: Key Chaining
FCS_TLS_EXT.1	Extended: TLS selected
FCS_SSH_EXT.1	Extended: SSH selected
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
FDP_RIP.1(a)	Subset residual information protection
FDP_RIP.1(b)	Subset residual information protection
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User attribute definition
FIA_PMG_EXT.1	Extended Password Management
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_PSK_EXT.1	Extended: Pre-Shared Key Composition
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization

Requirement	Title
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_KYP_EXT.1	Extended: Protection of Key and Key Material
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
FTA_SSL.3	TSF-initiated Termination
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1(a)	Trusted Path (for Administrators)
FTP_TRP.1(b)	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 1~~ Table 11**, [

- *Failure of HTTPS session establishment*
- *Failure of SSH session establishment*
- *Failure of TLS session establishment*
- *Failure to establish an IPSec SA*].

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 1~~ Table 11***, [*no other relevant information*].

Table 11: Audit Events

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

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_STG_EXT.1 Protected Audit Event Storage

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

FAU_STG.1 Protected Audit Trail Storage

FAU_STG1.1 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.

Application Note: FAU_STG.1 applies to local audit storage on the MFD.

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.

Application Note: FAU_STG.4 applies to local audit storage on the MFD.

5.3.2 Cryptographic Support (FCS)

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

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

- **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;**
- **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P256, P-384 and [P-521] (as defined in FIPS PUB 186-4, "Digital Signature Standard")**
- **NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes**

] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

FCS_CKM.1(b) Cryptographic Key Generation (Symmetric keys)

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

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

FCS_CKM.4(a) Cryptographic Key Destruction

FCS_CKM.4.1(a) 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 memory the destruction shall be executed by a [single] overwrite consisting of [*[0x35 or 0x97]*];

]
that meets the following: *No Standard*.

Application Note: This SFR is altered by TD0261.

FCS_COP.1(a) Cryptographic Operation (Symmetric Encryption/Decryption)

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

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

FCS_COP.1(b) Cryptographic Operation (for Signature Generation/ Verification)

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

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

that meets the following: [

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

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

FCS_COP.1.1(c) **Refinement:** The TSF shall perform **cryptographic hashing services** in accordance with [**SHA-1, SHA-256, SHA-384, SHA-512**] that meet the following: [**ISO/IEC 10118-3:2004**].

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

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [CBC] mode** and cryptographic key sizes **[256 bits]** that meet the following: **AES as specified in ISO/IEC 18033-3, [CBC as specified in ISO/IEC 10116]**.

Application Note: This SFR is for the FDP_DSK_EXT.1 requirement.

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

FCS_COP.1.1(g) **Refinement:** The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-[SHA-1, SHA-256, SHA-384, SHA-512], key size [*160, 256,***

***384, 512 bits*]**, **and message digest sizes [160, 256, 384, 512] bits** that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**

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

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

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

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 implement [tunnel mode, transport mode].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [the cryptographic algorithms

- AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC,
- AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC].

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

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [no other algorithm].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that: [IKEv1 SA lifetimes can be established based on [length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]]

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [no other DH groups].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [RSA] algorithm and Pre-shared Keys.

Application Note: This SFR is altered by TD0157

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 the HTTPS protocol using TLS as specified in FCS_TLS_EXT.1.

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_TLS_EXT.1 Extended: TLS selected

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

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_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
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA]

Application Note: This SFR is altered by TD0474.

FCS_SSH_EXT.1 Extended: SSH selected

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [6668].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_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_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [no other algorithms].

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [SSH_RSA] and [no other public key algorithms] as its public key algorithm(s).

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-512].

FCS_SSH_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1] and [no other methods] are the only allowed key exchange methods used for the SSH protocol.

Application Note: This SFR is altered by TD0494.

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 2 and Table3**~~ **Table 12 and Table 13.**

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 2 and Table3**~~ **Table 12 and Table 13.**

FDP_ACF.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in ~~Table 2 and Table3~~ Table 12 and Table 13.**

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

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

Table 12: D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	**Operation:**	**Submit a document to be printed**	**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**	**Release printed copy output**	**Modify stored image**	**Delete stored image**
	Job owner	(note 2) allowed	allowed	denied	denied
	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	denied
	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**	**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 13: D.USER.JOB Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	**Operation:**	**Create print job**	**View print queue/log**	**Modify print job**	**Cancel print job**
	Job owner	(note 1) 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
	Unauthenticated	denied	allowed	denied	denied

		"Create"	"Read"	"Modify"	"Delete"
Copy	**Operation:**	**Create copy job**	**View copy status/log**	**Modify copy job**	**Cancel copy job**
	Job owner	(note 2) allowed	allowed	denied	denied
	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 status/log**	**Modify fax send job**	**Cancel fax send job**
	Job owner	(note 2) allowed	allowed	denied	denied
	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(d)] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

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

FDP_FXS_EXT.1 Extended: Fax separation

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

FDP_RIP.1(a) Subset residual information protection

FDP_RIP.1.1(a) **Refinement:** The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting data** upon the **deallocation of the resource from** the following objects: **D.USER.DOC.**

FDP_RIP.1(b) Subset residual information protection

FDP_RIP.1.1(b) **Refinement:** The TSF shall ensure that any previous **customer-supplied** information content of a resource is made unavailable upon the **request of an Administrator to** the following objects: **D.USER, D.TSF.**

5.3.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [[*3*]] 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 [*lock the user for 5 minutes*].

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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [*and 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 [*asterisks*] 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, roles*].

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 1 to 32 characters*];

- composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

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

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 15*] 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 ~~Table 4~~ Table 14**.

Table 14: 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, delete	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 15*].

Table 15: 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, port and port range for remote trusted IT products (presumed) allowed to connect to the	X	X	X	X

Management Functions	Enable	Disable	Determine Behavior	Modify Behavior
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	

Application Note: Management functions in Table 15 are only accessible to system administrators.

FMT_SMR.1 Security Roles

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

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

5.3.6 Protection of the TSF (FPT)

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

FPT_KYP_EXT.1.1 **Refinement:** The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

FPT_SKP_EXT.1 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 a digital signature mechanism and [no other functions] prior to installing those updates.

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 path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 **Refinement:** The TSF shall **use [IPsec, SSH, TLS] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [authentication server, [*audit server, file server, mail server*]]** that is logically distinct from other communication channels and provides assured identification of its end

points and protection of the channel data from **disclosure and detection of modification of the channel data.**

FTP_ITC.1.2 **Refinement:** The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel.

FTP_ITC.1.3 **Refinement:** The TSF shall initiate communication via the trusted channel for [*user authentication, audit transmission, workflow scanning, scan to email*].

FTP_TRP.1(a) Trusted Path (for Administrators)

FTP_TRP.1.1(a) **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(a) **Refinement:** The TSF shall permit **remote administrators** to initiate communication via the trusted path.

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

FTP_TRP.1(b) Trusted Path (for Non-administrators)

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

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

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

5.4 Assurance Requirements

22 The TOE security assurance requirements are summarized in Table 16.

Table 16: TOE Security Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security Objectives for the operational environment
	ASE_REQ.1	Stated Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

6 TOE Summary Specification

6.1 Identification and Authentication

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

23 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.

24 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 12 and Table 13.

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

25 The TOE handles authentication failures as follows:

a) **EWS.** After three 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: "Login is currently locked: too many invalid login attempts. Please try again later." so 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 third failed attempt. Further login attempts do not extend this period.

b) **Control Panel.** After three successive failed attempts to login at control panel (i.e. the user acknowledged the error, and submitted incorrect data three 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 five minutes.

The control panel lockdown only applies to the Local UI. Therefore, if a user were locked out at the control panel, then EWS would still allow a user to log in.

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

26 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)

27 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.

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

29 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.

30 When a user enters a password, asterisks are displayed to obscure the password.

6.2 Security Audit

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

31 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.

32 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.

33 The TOE audit events are specified in Table 11 and the full list of auditable events can be found in Appendix A of the Xerox® AltaLink® Series Multifunction Printers System Administrator Guide. The TOE audit logs include a main audit log file and protocol log files.

6.2.2 Remote Audit Server (FAU_STG_EXT.1)

34 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)

35 The audit log may be downloaded from the MFP through EWS or the Control Panel. The System Administrator must be logged in to download the local audit log and is the only user with authorized access to the audit log.

36 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 Time (FPT_STM.1)

37 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, FMT_SMR.1)

38 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 bases on their role. Changes to user role are effective at the next user login.

39 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.

40 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)

41 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.

42 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 Copy

43 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, 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

6.3.2.2 Print

44 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.

45 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.

46 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.

6.3.2.3 Scan

47 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.

48 (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.

6.3.2.4 Fax

49 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). Once a job is submitted, 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).

50 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.

6.4 Security Management

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

51 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 15 for specific management functions.

52 As previously described, the TOE enforces a System Administrator defined role-based access control policy. Table 14 specifies the management of TSF data and what each role is permitted to do for TSF data.

6.5 Trusted Operation

6.5.1 Self-tests (FPT_TST_EXT.1)

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

a) **McAfee Embedded Control.** McAfee embedded control detects if critical executables have been modified by an extraneous method or non-updater ensuring that only authorized code can run, and only authorized changes can be made. If there are any attempts to change the system applications that operate the device, the administrator is alerted via email and an entry made into the audit log.

b) **Cryptographic Module Verification.** The OpenSSL and Mocana cryptographic modules each perform their own start-up integrity tests along with a suite of algorithm known answer tests. If any of the tests fail, the affected module will halt. Integrity tests are performed as follows:

   i) **Mocana.** The cryptographic module on initial invocation performs a HMAC-SHA2-256 software integrity test.

   ii) **OpenSSL.** The cryptographic module on initial invocation performs a HMAC-SHA-1 software integrity test.

54 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 modules.

6.5.2 Trusted Update (FPT_TUD_EXT.1)

55 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.

56 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(a), FCS_CKM.1(b), FCS_CKM.4(a), FCS_CKM_EXT.4, FCS_RBG_EXT.1, FPT_SKP_EXT.1)

57 The TOE cryptographic modules each implement random bit generation services using CTR_DRBG (AES) seeded with 256-bits of entropy from a hardware noise source as further described in the separate proprietary Entropy Description document.

58 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.

59 The TOE generates the following cryptographic keys:

a) FFC DH Group 14 (2048-bit MODP) per NIST SP 800-56Ar3 section 5.6.1.1.1

b) RSA 2048 per NIST SP 800-56Br2 section 6

c) ECDSA P256, P-384 and P-521 per NIST SP 800-56Ar3 section 5.6.1.2

d) 128-bit and 256-bit symmetric keys

60 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, when 'securely deleted' the material is overwritten with a single overwrite of the values (0x35 or 0x97). Table 17 below lists when key and key material are no longer needed.

61 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.

62 All private, pre-shared and symmetric keys stored on TOE removable storage areas are stored on encrypted partitions. The TOE uses AES-CBC-256 for all data encryption. See Table 17 for specific keys and their corresponding storage resource.

63 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 17: 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			
IPsec Private Key	RSA-2048	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	SHA-256 of Passphrase	Encrypted File System	AES-CBC-256	When a new pre-shared key is configured.

Key/CSP	Type / Strength	Storage	Protection	End-of-life / When key is destroyed
		RAM	n/a	Destroyed at power off.
IKE session authentication key	HMAC-SHA-1 HMAC-SHA2-256	RAM	n/a	Destroyed at power off.
IKE session encryption key	AES-128/256	RAM	n/a	Destroyed at power off.
IPSec session encryption key	AES-128/256	RAM	n/a	Destroyed at power off.
IPSec session authentication key	HMAC-SHA-1 HMAC-SHA2-256	RAM	n/a	Destroyed at power off.
SSH Private Key	RSA-2048	Encrypted File System	AES-CBC-256	When generating a new keypair.
		RAM	n/a	Destroyed at power off.
SSH Session Authentication Key	HMAC-SHA-1/96 HMAC-SHA2-512	RAM	n/a	Destroyed at power off.
SSH Session Encryption Key	AES-128/256	RAM	n/a	Destroyed at power off.
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)	Password	Encrypted File System	AES-CBC-256	n/a as passwords are hashed and salted.

6.6.2 Encryption/Decryption (FCS_COP.1(a), FCS_COP.1(d))

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

a) AES-CBC-128/256 for TLS, IPsec and SSH

b) AES-GCM-128/256 for TLS

c) AES-CBC-256 for disk encryption

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

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

a) RSA 2048 (FIPS 186-4)

b) ECDSA P-256, P384, P521 (FIPS 186-4)

6.6.4 Hashing Services (FCS_COP.1(c), FCS_COP.1(g))

66 The TOE provides cryptographic hashing services using SHA-1, SHA2-256, SHA2-384, and SHA2-512. SHA is used in:

a) TLS

b) IPsec

c) SSH

d) Trusted Update (digital signature verification)

e) Storage Encryption

67 The TOE implements HMACs as shown Table 18. HMAC is used in:

a) TLS

b) IPsec

c) SSH

Table 18: HMAC Characteristics

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA-1	512 bits	160 bits	160 bits
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

68 Table 19 provides a mapping between the SFRs and CAVP certificates. The TOE incorporates two cryptographic modules:

a) **Mocana Cryptographic Library v6.4.1f.** Provides cryptographic services for storage encryption, IPSec and all asymmetric key generation (including RSA and ECDSA keys used in TLS).

b) **OpenSSL FIPS Object Module v2.0.11.** Provides cryptographic services for HTTPS/TLS and SSH encryption/decryption. **Note:** This module is also identified as “Xerox OpenSSL v1.1” in the CAVP certificate RSA 2690. They are the same module.

Table 19: CAVP Certificate Mapping

SFR	Capability	OpenSSL	Mocana
FCS_CKM.1(a)	RSA Key Gen (186-4)	n/a	RSA 2296
	ECDSA Key Gen (186-4)	n/a	ECDSA 994
	DSA Key Gen (186-4)	n/a	DSA 1140
FCS_CKM.1(b) FCS_RBG_EXT.1	Counter DRBG	DRBG 845	DRBG 1336
FCS_COP.1(a) FCS_COP.1(d)	AES (CBC, GCM)	AES 3451	AES 4265
FCS_COP.1(b)	RSA SigGen/SigVer (186-4)	RSA 2690	RSA 2296
	ECDSA SigGen/SigVer (186-4)	ECDSA 698	n/a
FCS_COP.1(c)	SHA-1, SHA2	SHS 2847	SHS 3511
FCS_COP.1(g)	HMAC	HMAC 2197	HMAC 2810

6.7 Storage Encryption

6.7.1 Disk Encryption (FDP_DSK_EXT.1)

69 Disk encryption is enabled by default at the factory when the device is first delivered.

70 All files and meta data for the file system will be written in blocks by the file system code, those block are passed through a block i/o driver to loopaes, which then encrypts each block sending the encrypted block to the hard disk drive controller driver that sends it to the disk drive controller. The file system doesn't know about encryption, it just reads and writes the disk blocks and loopaes takes care of the encrypting/decrypting to/from the hard drive.

71 User writes file data -> file system writes data in blocks -> loopaes gets block and encrypts -> drive block controller writes block (which is encrypted data) to disk drive

72 The device does not encrypt data in these partitions named: boot, root, opt, and swap. Details on encrypted partitions are in the KMD.

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

73 The TOE generates a 256-bit BEV for disk encryption. 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(a), FTP_TRP.1(b))

74 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)

75 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.

76 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.

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

6.8.3 TLS (FCS_TLS_EXT.1)

78 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 (SMTPS) and Workflow Repository File Server (HTTPS).

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

a) TLS_RSA_WITH_AES_128_CBC_SHA

b) TLS_RSA_WITH_AES_256_CBC_SHA

c) TLS_DHE_RSA_WITH_AES_128_CBC_SHA

d) TLS_DHE_RSA_WITH_AES_256_CBC_SHA

e) TLS_RSA_WITH_AES_128_CBC_SHA256

f) TLS_RSA_WITH_AES_256_CBC_SHA256

g) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

h) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

i) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

j) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

k) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

l) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

m) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

n) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

o) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

p) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

q) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

r) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

s) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

t) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

80 TLS client authentication is not supported.

6.8.4 SSH (FCS_SSH_EXT.1)

81 SSH/SFTP is used to transfer audit logs to a remote log server. The TOE SSH client supports the following:

a) Public key and password-based authentication is supported

b) Packets greater than 40,000 bytes are dropped

c) Transport encryption supports aes128-cbc and aes256-cbc

d) Supported public key algorithms: ssh_rsa.

e) Supported data integrity algorithms: hmac-sha1, hmac-sha1-96, hmac-sha2-512

f) Supported key exchange methods include Diffie-hellman-group14-sha1

82 There is no configuration at the TOE to restrict or select any of the above characteristics other than the authentication method. The TOE will indicate to the server in SSH negotiation sequences that all above algorithms are supported in SSH protocol handshaking and will accept any of the above that the server selects.

83 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)

84 The TOE uses IPsec for communication with a Domain Controller for Smart Card authentication and to protect communication with all remote print clients.

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

86 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. Unless configured otherwise, for any packet not fitting any of the defined polices, the default action is to bypass (pass through) the packet.

87 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 by default 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. The evaluated configuration is set up in order to test all possible actions of bypass, drop, and applied cryptography.

88 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.

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

90 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-SHA1, HMAC-SHA2-256.

91 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.

92 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), is the only DH group allowed.

93 The TOE can be configured to perform peer authentication using RSA certificates along the DH mode configured (DH group 14) during IKE Phase 2. If the TOE is configured to use RSA, 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 RSA digital certificates or pre-shared keys for peer authentication by creating an IP policy rule in the TOE's IP Security Policy.

94 The pre-shared key is configurable with an ASCII text string with range of 1 – 32 octets. This includes the construction of the 22 octet length pre-shared key. The entry of the pre-shared key is masked so that onlookers will not see the values, and the values cannot be displayed at any time. 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)

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

96 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.

97 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.

98 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 Image Overwrite (FDP_RIP.1(a))

99 The TOE implements Image Overwrite security function (using a three pass overwrite procedure consistent with U.S. Department of Defense National Industrial Security Program Operating Manual – DoD 5220.22-M – requirements) to overwrite all temporary files created during processing of jobs, files (images) of completed or deleted jobs or any files that are deleted.

100 The TOE spools and processes documents to be printed or scanned. Temporary files are created as a result of this processing on a reserved section of the hard disk drive. The definition of this reserved section is statically stored within the TOE and cannot be manipulated. Immediately after the job has completed, the files are overwritten, and this is called Immediate Job Overwrite.

101 The TOE automatically starts a Immediate Job Overwrite procedure for all abnormally terminated copy, print, scan or fax jobs stored on the HDD prior to coming “on line” when any of the following occurs: a reboot or once the MFD is turned back on after a power failure/disorderly shutdown.

102 The Immediate Image Overwrite security function can also be invoked manually by the system administrator. Once invoked, the Immediate Job Overwrite feature cancels all jobs, halts the printer interface (network), performs the overwrites, and then the network controller reboots. A scheduling function allows Image Overwrite to be executed on a recurring basis as set up by the System Administrator.

103 A standard Image overwrite, overwrites all files written to temporary storage areas of the HDD. A full Image overwrite, overwrites those files as well as the Fax mailbox/dial directory and Scan to mailbox data.

104 A Immediate Job Overwrite cannot be aborted from either the EWS or Local UI. For entire duration of process, EWS and Local UI is offline and no user interaction available.

105 The Image Overwrite function overwrites the contents of the reserved section on the hard disk using a three pass overwrite procedure.

6.10.2 Purge (FDP_RIP.1(b))

106 The purge function is invoked manually by the system administrator. Once invoked, the purge function overwrites all jobs that are actively being processed by the TOE or are being held on the TOE for later processing; overwrites all jobs and log files that are stored on the hard drive(s); overwrites all local authentication data stored on the internal database; overwrites all customer data stored in address books and accounting databases and resets the fax and copy controller NVM on the TOE to their factory default values. At the completion of the purge function the TOE will reformat the hard drive(s), print a confirmation page, reboots the TOE and re-install the system software release that was installed on the TOE when the purge function was invoked.

7 Rationale

107 This ST includes security rationale by reference to the Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015. The ST makes no additions to the PP defined Security Problem Definition or Security Objectives, and all security requirements have been reproduced from the PP with the PP operations completed. Operations on the security requirements follow the PP application notes and assurance activities. Consequently, the PP rationale applies.