Xerox Multi-Function Device Security Target

Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD

Xerox Corporation
800 Phillips Road
Webster, New York 14580

August 2021
Version 0.6

Table of Contents

List of Figures

List of Tables

1. Introduction

This Security Target (ST) specifies the security claims of the C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD in accordance with the requirements of the Common Criteria (CC).

The TOE is equipped with a Solid-State Drive (SSD). Purchasers that require NIST SP 800-88Rev1 conformant Image Overwrite (IIO/ODIO) functionality should use the TOE Xerox Altalink C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD which implements traditional overwrite functionality that is not possible with SSD technology.

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE identification, ST and TOE conformance claims, ST conventions, glossary and list of abbreviations.

- TOE Description (Section 2) — provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3) — describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4) — describes the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions that define the security problem
- IT Security Requirements (Section 5) — specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 6) — describes the security functions of the TOE and how they satisfy the SFRs
- Rationale (Section 7) — provides mappings and rationale for the security problem definition, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.
- Glossary (Section 8) — terms that have a specific meaning within the context of the ST and the TOE.
- Acronyms (Section 9) — abbreviations and acronyms that are used in this document.

1.1 ST and TOE Identification

Table 1 below presents key identification details relevant to the CC evaluation of the Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8075 with SSD TOE.

Table 1: ST and TOE identification

ST Title:	Xerox Multi-Function Device Security Target, Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8075 with SSD
ST Version:	0.6
April	August 2021
Authors:	Xerox Corporation
TOE Identification:	Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8075 with SSD System Software version: 111.011.000.27020 and 111.013.000.27020
ST Evaluator:	CCTL
Keywords:	Xerox, Multi-Function Device, WorkCentre, Printer, Scanner, Copier, Facsimile, Fax, Document Server, Document Storage and Retrieval, All-In-One, MFD, MFP, ISO/IEC 15408, Common Criteria, FIPS, Protection Profile, Security Target

1.2 Conformance Claims

This ST supports the following conformance claims:

- CC version 3.1 revision 5
- CC Part 2 extended
- CC Part 3 conformant
- Protection Profile for Hardcopy Devices, v1.0
- Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017
- NIAP Technical Decisions listed below

1.2.1 Profile Claims

This ST and the TOE it describes are conformant to the following Protection Profile:

- Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015 ([HCDPP]). The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:
  - 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 (does not apply as the TOE does not claim FCS_COP.1(i))
  - 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
- TD0494: Removal of Mandatory SSH Ciphersuite for HCD
- TD0562: Test Activity for Public Key Algorithms

1.2.2 Package Claims

None.

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements—Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement. The conventions used in the PP to identify these operations are replicated in this security target.
  - Iteration: allows a component to be used more than once with varying operations. In this ST, iteration is represented by a letter in parantheses placed at the end of the component. For example, FCS_CKM.1(a) and FCS_CKM.1(b) indicate that the ST includes two iterations of the FCS_CKM.1 requirement.
  - Assignment: allows the specification of an identified parameter. Assignment operations that are completed in the PP are represented using bolded text. Assignment operations that are completed in the ST are indicated using italic. Note that an assignment within a selection would be identified with bold italic.
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using italics.
  - Refinement: allows the addition of details. Refinements are indicated using bold for additions and strike-through for deletions (e.g., "… **all objects** …").
  - Extended components are identified by "_EXT" appended to the SFR identifier.
- Other sections of the ST—other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Overview

2.1 TOE Description

The Target of Evaluation (TOE) is the Xerox multi-function device (MFD) Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8075 with SSD. The TOE copies and prints with scan and fax capabilities. The Xerox Embedded Fax Accessory provides local analog fax capability over Public Switched Telephone Network (PSTN) connections and also enables LanFax[1].

Xerox's Workflow Scanning Accessory allows documents to be scanned at the device with the resulting image being sent via email, transferred to a remote file repository or kept in a private (scan) mailbox.

The TOE can integrate with an IPv4 network with native support for DHCP. The hardware included in the TOE is shown in the figure below.

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

In addition to the LUI, user may also interact with the TOE via the EWS also referred to as Embedded Web Server, 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.

TOE Architecture

Figure 1: Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8075

[1] LanFax enables fax jobs to be submitted from the desktop via printing protocols.

2.1.1 Physical Boundary

The TOE is an MFD (Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD) that consists of a printer, copier, scanner, fax and associated administrator and user guidance. The TOE comprises the hardware, all software and firmware within the MFD enclosure.

Xerox® AltaLink® B8145/B8155/B8170 are mono MFP or black and white printers; C8130/C8135/C8145/ C8155/C8170 are color MFP or color printers. All models have an Intel Atom E3950 (Goldmont) processor and run WindRiver Linux 9.0. Each model consists of an input document handler and scanner, Xerox embedded Fax accessories, marking engine, controller, Xerox Worflow scanning accessory and user interface. Differences between models is limited to print speed and options such as finishers, paper trays and document handlers. The differences between the models are not security relevant.

The Xerox MFP's within the scope of the evaluation are shown in the table below.

Table 2: Xerox MFP's

Model	Firmware Version	CPU / OS
AltaLink™ C8130 / C8135 C8145 / C8155/ C8170	111.011.000.27020	Intel Atom E3950 (Goldmont) Wind River Linux 9.0
AltaLink™ B8145 / B8155/ B8170	111.013.000.27020	

2.1.2 TOE Documentation

The TOE documentation and guidance documents are listed in Table 3.

Table 3: TOE Documentation and Guidance

Title	Version	Date
Xerox® AltaLink® Series Multifunction Printers System Administrator Guide	2.4	February 2021
Xerox® AltaLink® B81XX Series Multifunction Printer User Guide	1.0	May 2020
Xerox® AltaLink® C81XX Series Color Multifunction Printer User Guide	1.0	May 2020
Xerox® AltaLink® Series Smart Card Installation and Configuration Guide	3.0	December 2020
Secure Installation and Operation AltaLink B81xx C81xx Guidance	2.2	August 2021
Xerox Altalink 81xx MFP Key Management Description	3.0	August 2021
Xerox AltaLink 81xx MFP Entropy Description	1.0	January 2021

2.1.3 Logical Boundary

The TOE provides the following security features:

2.1.3.1 Identification and Authentication

In the evaluated configuration, the TOE requires users and system administrators to authenticate before granting access to user (copy, print, fax, etc.) or system administration functions via the Embedded Web Server (EWS) or the Local User Interface (LUI). The user or system administrator must enter a username and password at either the EWS or the LUI. The password is obscured as it is being entered. The TOE provides role based access control as configured by the system administrator.

The TOE also supports smart card and Lightweight Directory Access Protocol (LDAP) for network authentication.

2.1.3.2 Security Audit

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to identified users. The audit logs, which are stored locally in a 15000 entry circular log, are available to TOE administrators and can be exported in comma separated format for viewing and analysis.

2.1.3.3 Access Control

The TOE enforces a system administrator defined role based access control policy. Only authenticated users assigned to roles with the necessary privileges are allowed to perform copy, print, scan or fax on the TOE via the EWS or the LUI.

Unauthenticated users can submit print or LanFax jobs to the TOE via printing protocols. Release of unauthenticated print jobs to the hardcopy output handler is dependent on the system administrator defined policy.

2.1.3.4 Security Management

A Local User, via the local user interface, or a Remote User, via EWS, with administrative privileges can configure the security settings of the TOE. The TOE has the capability to assign Users to roles that distinguish Users who can perform administrative functions from Users who can perform User functions via a role based access control policy. The TOE also has the capability to protect its security settings from unauthorized disclosure and alteration when they are stored in the TOE and in transit to or from the browser-based interface.

2.1.3.5 Trusted Operation

The TOE includes a software image verification feature and Embedded Device Security which it uses to detect unauthorized modification of TOE software and to verify correct operation of the TOE software.

2.1.3.6 Encryption

The TOE includes the Mocana cryptographic module software version 6.5.1f (See Table 15 for CAVP certificates) which it uses for all in-scope cryptographic operations. The TOE utilizes digital signature generation and verification (RSA), data encryption (AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC) in support of disk encryption, SSH, TLS, TLS/HTTPS, TLS/SMTP

and IPsec. The TOE also provides random bit generation in support of cryptographic operations.

The TOE stores temporary image data created during a copy, print, scan and fax job on the single shared solid disk drive (SSD). This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the SSD used for spooling temporary files are encrypted. All print scan, and fax jobs are sent over IPSec encrypted channels. The SSD drive encryption key is derived from a BIOS saved passphrase and is the same value for each power-up (see KMD for details.)

2.1.3.7 Trusted Communication

The TOE provides support for a number of secure communication protocols:

- Transport Layer Security (TLS) support is available for protecting communication over the Embedded Web Server (EWS) and SMTP email communications. TLS is also used to protect communication with the remote authentication server (LDAPS)
- Secure Shell (SSH) File Transfer Protocol (SFTP) is available for audit log secure transfers to a remote file repository.
- Internet Protocol Security (IPsec) support is available for protecting communication with print clients and communication with the domain controller when using SmartCard authentication.

2.1.3.8 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.

2.1.3.9 Data Clearing and Purging (Job data Removal)

The purge (also known as Job Data Removal) 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.

2.1.4 Features not tested

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

- Reprint from Saved Job
- SMart eSolutions
- Custom Services (Extensible Interface Platform or EIP)
- Network Accounting and Auxiliary Access
- Internet Fax
- Embedded Fax mailboxes
- Wi-Fi Direct Printing
- Weblet Services
- InBox Apps

- Remote Control Panel
- SFTP when used for scanning
- SNMPv3
- Scan to USB
- Print from USB
- SMB Filing
- Convenience Authentication
- Xerox Workplace Cloud
- Proximity Card Authentication

2.2 Required Non-TOE Components

The TOE operates with the following components in the environment:

- IPv4 or IPv6 network environment
- Publicly Switched Telephone Network (PSTN)
- LDAP server for external authentication services
- NTP server for time services
- File server for Workflow Scanning
- Log server (file server) for remote log storage
- Printer drivers on supported OS per https://www.support.xerox.com/support/altalink-c8100-series/support/enus.html
- 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.

3. Security Problem Definition

The security problem definition consists of the threats, organizational security policies, and usage assumptions as they relate to the TOE.Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8075 The Security Problem Definition is reproduced from the HCDPP.

3.1 Threats

Table 4: HCD PP Threats addressed

ID	Threats
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.2 Assumptions

Table 5: HCD PP Assumptions addressed

ID	Assumptions
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 6: HCD PP OSPs addressed

ID	Organizational Security Policy
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.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

The Security Objectives have been taken from the [HCDPP] and are reproduced for the convenience of the reader.

4.1 Security Objectives for the TOE

Table 7: HCD PP Security Objectives addressed

ID	Security Objective for the TOE
O.USER_I&A	The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles.
O.ACCESS_CONTROL	The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
O.USER_AUTHORIZATION	The TOE shall perform authorization of Users in accordance with security policies.
O.ADMIN_ROLES	The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.
O.UPDATE_VERIFICATION	The TOE shall provide mechanisms to verify the authenticity of 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.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 8: Security Objectives for the Operational Environment

ID	Security Objective for the Operational Environment
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. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that represent the security claims for the Target of Evaluation (TOE) and scope the evaluation effort.

All the SFRs have been drawn from HCDPP. As such, operations already performed in that PP are not identified here. Instead, the requirements have been copied from the PP and any incomplete selections or assignments have been performed herein. Of particular note, the PP makes a number of refinements and completes some SFR operations defined in the CC, so it should be consulted if necessary to identify those changes.

The SARs are the set of SARs specified in [HCDPP].

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [HCDPP]. The [HCDPP] defines the following extended SFRs and since they are not redefined in this ST, the [HCDPP] should be consulted for more information in regard to those CC extensions.

- **FAU_STG_EXT.1: Extended**: External Audi Trail Storage
- **FCS_CKM_EXT.4: Extended**: Cryptographic Key Destruction
- **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_SSH_EXT.1: Extended:** SSH selected
- **FCS_TLS_EXT.1: Extended:** TLS selected
- **FIA_PSK_EXT.1: Extended:** Pre-Shared Key Composition
- **FCS_KYC_EXT.1 Extended:** Key Chaining
- **FIA_PMG_EXT.1: Extended**: Password Management
- **FPT_SKP_EXT.1: Extended**: Protection of TSF Data
- **FPT_TST_EXT.1: Extended**: TSF Testing
- **FPT_TUD_EXT.1: Extended**: Trusted update
- **FPT_KYP_EXT.1 Extended:** Protection of Key and Key Material
- **FDP_DSK_EXT.1 Extended:** Protection of Data on Disk
- **FDP_FXS_EXT.1 Extended:** Fax separation

5.2 Security Functional Requirements

5.2.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) **All auditable events specified in ~~Table 1~~ Table 9**, [*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 9,** [*no other relevant information].*

Table 9: Auditable Events

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

5.2.2 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.

5.2.3 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

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

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

5.2.4 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% full*] if the audit trail is full.

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

5.2.5 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.

5.2.6 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.

5.2.7 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.

5.2.8 FCS_CKM.4 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.

5.2.9 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.

5.2.10 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*]

5.2.11 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 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").].

5.2.12 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-256, SHA-384, SHA-512*] that meet the following: **[ISO/IEC 10118-3:2004].**

5.2.13 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.*

5.2.14 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-256, SHA-384, SHA-512***], key size [***256, 384, 512 bits***], and message digest sizes **[*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."**

Application Note*: This SFR is for the FCS_IPSEC_EXT.1.4 requirement.*

5.2.15 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.

5.2.16 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 [*19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP))*].

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.*

5.2.17 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_TLS_EXT.1.

***Application Note**: HTTPS is used by FTP_TRP.1(a) and FTP_TRP.1(b) for print transmitted to and from the TOE and for administrator management of the TOE.*

5.2.18 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*] while maintaining an effective strength of [*256 bits*].

5.2.19 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_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384].*

***Application Note**: This SFR is altered by TD0474.*

5.2.20 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, ecdsa-sha2-nistp256]* and *[ecdsa-sha2-nistp384]* 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-SHA2-256*, *HMAC-SHA2-512*].

FCS_SSH_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.

Application Notes*:* This SFR is altered by TD0494.

5.2.21 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 Table 3~~ Table 10 and Table 11.

5.2.22 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 Table 3~~ Table 10 and Table 11.

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 Table 3~~ Table 10 and Table 11.

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 10: 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

		"Create"	"Read"	"Modify"	"Delete"
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***
	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 11: 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
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***

		"Create" *	"Read"	"Modify"	"Delete"
	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.*

See also the following Notes that are referenced in Table 10 and Table 11:

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.*

5.2.23 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.

5.2.24 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.

5.2.25 FDP_RIP.1(b) Subset residual information protection

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

5.2.26 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 the EWS or local UI*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*surpassed*], the TSF shall *[lock the user for 5 minutes].*

5.2.27 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*].

5.2.28 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.

5.2.29 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.

5.2.30 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.

5.2.31 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.

5.2.32 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 is 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*].

5.2.33 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*].

5.2.34 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 **Refinement:** The TSF shall restrict the ability to [*determine the behavior of, disable, enable, modify the behavior of*] the functions [*functions listed in Table 13*] to U.ADMIN.

5.2.35 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].

5.2.36 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.

5.2.37 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 12.**

Table 12: Management of TSF Data

Data	Operation	Authorised 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 the EWS or the Local UI.	query	U.NORMAL (Authenticated user)
Authenticated user roles to copy, print, scan or fax on the TOE via the EWS or the Local UI.	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

5.2.38 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following management function: [*Management functions listed in Table 13*].

Table 13: Management Functions

Management Functions	Enable	Disable	Determine Behavior	Modify Behavior
Enable/disable and configure smart card use	X	X	X	
Manage receive fax (job) passcodes			X	
Configure EWS and LUI 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 TOE via the network interface) IP filtering	X	X	X	X
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	
Invoke data purge function (Job Data Removal)	X	X		
Enable/disable and configure fax forwarding to email	X	X	X	
Configure Software/Firmware update	X	X		
Configure NTP	X	X	X	
Configure STARTTLS	X	X	X	

Application Note: All management functions in Table 13 are only accessible to system administrators.

5.2.39 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.

Application Note: *U.ADMIN role applies to user with System Administrator permissions. U.NORMAL applies to other authenticated users.*

5.2.40 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.**

5.2.41 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.

5.2.42 FPT_STM.1 Reliable time stamps

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

5.2.43 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.

5.2.44 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.

5.2.45 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:*

- *the Local UI will terminate any session that has been inactive for 1 minute;*
- *the EWS will terminate any session that has been inactive for 60 minutes].*

5.2.46 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall use **[***SSH, TLS, IPsec***]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities:** *[authentication server, [audit server, file 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 [*audit transmission and user authentication service*].

5.2.47 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**.

***Application Note**: This is only for the use of remote management functions over the Embedded Web Server.*

5.2.48 FTP_TRP.1(b) Trusted path (for non-administrators)

FTP_TRP.1.1(b) Refinement: The TSF shall use **[***IPsec, TLS, and 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 and 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**.

***Application Note**: This includes sending secure print jobs, scan jobs, and mailbox retrieval for any remote user.*

5.3 Security Assurance Requirements

This section specifies the SARs for the TOE. The SARs are included by reference from [HCDPP].

Table 14: Assurance Components

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction

Assurance Class	Components	Description
	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

This section presents an overview of the security functions implemented by the TOE.

6.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Sections 5.2.

- Identification and Authentication
- Security Audit
- Access Control
- Security Management
- Trusted Operation
- Encryption
- Trusted Communication
- PSTN Fax-Network Separation
- Data Clearing and Purging

6.1.1 Identification and Authentication

FIA_AFL.1	**EWS Login** 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: "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 fifth failed attempt. Further login attempts do not extend this period. **Local UI Login** After five successive failed attempts to login at Local UI (i.e. the user acknowledged the error, and submitted incorrect data five times without canceling out of the authentication process) the device shall lockdown Local UI Authentication. The Local UI shall continue to display the login prompt after the lockdown has been initiated All attempts to login at the Local UI shall fail after the lockdown has been initiated, even if a valid username and password are provided

	The Local UI lockdown shall last for five minutes. The Local UI lockdown only applies to the Local. Therefore, if a user were locked out at the LUI, then EWS would still allow a user to log in. The Local UI lockdown shall not impact a user's ability to access Local UI 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
FIA_ATD.1	The TOE maintains username and password credentials for each authenticated user and associated roles configured for the authenticated user. The TOE uses both an internal user database and external LDAP servers for user authentication.
FIA_PMG_EXT.1	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. The maximum Password field length is limited by the device to a string of 63 octets (plus NULL1). The 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.
FIA_UAU.1, FIA_UID.1	The TOE provides the following means to identify and authenticate to the TOE: **Local Authentication —** The TOE uses a local information database for users accessing through the Local UI (operation panel) and EWS (browser based). **Network Authentication —** The TOE uses LDAP to identify and authenticate users accessing through the Local UI and the EWS. **Smartcard Authentication –** 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. 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 10 and Table 11.

FIA_UAU.7	When a user enters passwords at the EWS or Local UI, asterisks are displayed rather than the entered character in order to obscure password.
FIA_USB.1	The TOE assigns each user one or more roles in the system. 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.
FTA_SSL.3	By default, the LUI 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 LUI and EWS session timeouts to terminate an inactive session after some other period of time.

6.1.2 Security Audit

FAU_GEN.1, FAU_GEN.2	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), changes to the time, and failure of trusted channels. 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. The audit events are specified in Table 9 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.
FAU_STG_EXT.1	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. Configuring the transfer or using the 'send now' feature is available via TOE EWS only.
FAU_STG.1	The audit log may be downloaded from the MFP through the EWS or the LUI. The system administrator must be logged in

	to download the audit log and is the only user with authorized access to the audit log.
FAU_STG.4	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.
FPT_STM.1	During initial device configuration the initial date and time are set. The TOE maintains the date and time to provide reliable timestamps. The TOE also can be configured to to synchronize time with an NTP server in the operational environment.

6.1.3 Access Control

FDP_ACC.1, FDP_ACF.1	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 Local UI: • Print • Scan • Fax (receive and send) • Copy Any User who is authorized to establish a connection with the TOE through the ethernet port is able to perform the following TOE functions: • **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. • **Scan -** Any host / authorized user on the network can submit Scan jobs. • **Fax -** Any host / authorized user on the network can submit LanFax jobs. • **Copy -** Any host / authorized user on the network can submit copy jobs.

6.1.4 Security Management

FMT_MOF.1, FMT_SMF.1	All management functions are only usable by the System Administrator. The System Admistrator specifies whether management functions can be enabled, disabled, and determines or modifies the behavior of the function. The System administrator also limits any management functions to specified user level access. See Table 13 for specific Management functions.
FMT_MSA.1, FMT_MSA.3	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. **Copy** 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 **Print** 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. 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.

	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. **Scan** 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. (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. **Fax** 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). 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.
FMT_MSA.1, FMT_MTD.1, FMT_SMR.1	Table 12 specifies the management of TSF data and what each role is permitted to do for the TSF data. The TOE enforces a system administrator defined role based access control policy. Only authenticated users assigned to roles with the necessary privileges are allowed to perform copy, print, scan or fax on the TOE via the EWS or the LUI.

	The TOE maintains two roles, U.NORMAL and U.ADMIN. Authenticated user roles and permissions can only be modified by a U.ADMIN user with System Administrator permissions. Authenticated users may only change their password, as they cannot see the EWS options or the LUI pathways for configuring and managing the TOE functions and TSF data. The TOE implements a role based access control system. The TOE ships with two pre-configured roles: • **System Administrator.** Has access to all pathways, services and features including all management functions on the TOE. • **Authenticated 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. Only an admistrator is allowed full access to the TOE including all the system administrator functions.

6.1.5 Trusted Operation

FPT_TST_EXT.1	The TOE includes the Mocana cryptographic module (Table 15 below identifies the CAVP certificates relevant to the TOE cryptographic functions) The TOE performs a set of self-tests during startup which includes the following: **Trusted Boot** Intel's Boot Guard runs trusted firmware from the internal boot ROM. The TOE begins execution with a hardware-based root of trust. Boot Guard's first function is to use a pre-determined digital signature to verify the initial startup microcode is authentic and unmodified, by verifying that the signature hash is correct. The chain of trust is passed on to the UEFI image which verifies the OS Boot Manager. The OS Boot Manager verifies the boot objects up to and including McAfee as well as the installation objects. On failure the device halts and when possible displays a Post Code. **McAfee Embedded Control** The McAfee standard installation detects if critical executables have been modified by an extraneous method or non-updater. Allows only authorized code to be run and authorized changes to 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. **Cryptographic Module Verification** The cryptographic module on initial invocation performs a HMAC-SHA-256 software integrity test and halts if the tests fails. During the load of the shared object at startup, the integrity check of the library code and constants occurs in the module startup function. It verifies the integrity by executing the HMAC-SHA 256 fingerprint algorithm on the shared library .so file, and comparing the result with the signature file. 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. Together, the above tests are sufficient to demonstrate that the TSF is operating correctly by verifying the TSF's code authenticity and integrity along with verifying the correct operation of the cryptographic module.
FPT_TUD_EXT.1	The TOE provides a EWS page that shows the Software Version, allows a print of the Configuration Report which contains the Software Version and Local UI access to display the Software Version. The EWS provides a System Administrator the function to upgrade the software image. Image files are encrypted using the AES 256 cipher. The key that was used to encrypt with AES 256 is encrypted itself by use of a RSA 2048 bit private key. The encrypted image file is hashed and signed using the SHA-256 hash cipher, and a protected, non user accessible RSA 2048 bit private key. On the TOE, prior to image installation, the corresponding RSA 2048 bit public key is used to decrypt the hash and the SHA 256 cipher is used to verify the hash. The TSF performs signature verification on software upgrade image prior to performing the update. If the signature verification fails, the upgrade will be aborted
FPT_SKP_EXT.1	All private, pre-shared and symmetric keys stored on TOE removable storage areas are encrypted as a result of the partitions on which they reside on being encrypted, or both. The TOE uses AES-CBC-256 for all data encryption. See Table 16 for specific Keys and their corresponding storage resource.

	The TOE does not allow the user, either of admin, or non-admin privileges, through any customer provided interface to view, or obtain any pre-shared key, private key, or symmetric key.

6.1.6 Encryption

FCS_CKM.1(a) FCS_CKM.1(b)	The TOE includes the Mocana Cryptographic library version 6.5.1f which it uses for all cryptographic services. Table 15 below identifies the CAVP certificates for the TOE cryptographic Services. The TOE uses CTR-DRBG to generate cryptographic keys. 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. The TOE generates the following cryptographic keys: • FFC DH Group 14 (2048-bit MODP) per NIST SP 800-56Ar3 section 5.6.1.1.1 • RSA 2048 per NIST SP 800-56Br2 section 6 • ECDSA P256, P-384 and P-521 per NIST SP 800-56Ar3 section 5.6.1.2 • 128-bit and 256-bit symmetric keys • The KMD document provides additional information on key generation and on invoking the DRBG.
FCS_CKM.4 FCS_CKM_EXT.4	Keys and keying material when no longer used or replaced are securely deleted. 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 16 below lists when key and key material are no longer needed. Key destruction is further described in a separate proprietary Key Management Document. There are no known configurations or circumstances that do not conform to the key destruction requirements.
FCS_COP.1(a) FCS_COP.1(d)	For encryption/decryption services, 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-256 for disk encryption
FCS_COP.1(b)	The supports the following digital signature generation and verification services: • RSA 2048 (FIPS 186-4)

	• ECDSA P-256, P384, P521 (FIPS 186-4)
FCS_COP.1(c)	The TOE provides cryptographic hashing services using SHA-256, SHA-384, and SHA-512. SHA is used in: • TLS • IPsec • SSH • Trusted Update (digital signature verification)
FCS_COP.1(g)	The TOE implements HMACs as shown Table 19. HMAC is used in: • TLS • IPsec • SSH
FCS_RBG_EXT.1	The TOE implements random bit generation services using CTR_DRBG (AES) seeded with at least 256-bits of entropy from a hardware noise source as further described in the separate proprietary Entropy Description document.
FPT_KYP_EXT.1, FCS_KYC_EXT.1	The TOE generates a 256-bit BEV for disk encryption. The BEV is not stored in plaintext. Further details are provided in a separate proprietary Key Management Document.
FDP_DSK_EXT.1	Disk encryption is enabled by default at the factory when the device is first delivered. 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. 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 The device does not encrypt data in these partitions named: boot, root, opt, and swap. Details on encrypted partitions are in the KMD.

Table 15: SFRs and CAVP certificates

SFR	CAVP certificate
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)	CVL# 1723 RSA# 2809 DRBG# 2009 SHS# 4229

FCS_CKM.1(b) Cryptographic Key Generation (for symmetric keys)	DRBG# 2009
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)	AES# 5252, 5253, 5254
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)	RSA# 2809 ECDSA# 1368 DSA# 1360
FCS_COP.1(c) Cryptographic operation (Hash Algorithm)	SHS# 4229
FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)	AES# 5252
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)	HMAC# 3478
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)	DRBG# 2009

Links to specific Mocana security module CAVP certificates:

https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=9193

https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=9195

https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=9196

Table 16: Keys and CSPs

Key/CSP	Type / Strength	Storage	Protection	End-of-life / When key is destroyed
IPsec 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	SHA-256 of Passphrase	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-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-256/512	RAM	n/a	Destroyed at power off.

Key/CSP	Type / Strength	Storage	Protection	End-of-life / When key is destroyed
SSH Private Key	RSA-2048 ECDSA-P256/P384	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/P512	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-SHA-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)	SHA-256	Encrypted File System	AES-CBC-256	When a user changes their password. When a user is deleted.

Table 17: HMAC Characteristics

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

6.1.7 Trusted Communication

FTP_ITC.1	The TOE supports the following protocol for secure communication with external IT entities: • TLS for document transfers to a remote file repository, for SMTP communication and for communication with a remote authentication server (LDAPS) • SSH for audit log transfer to a remote log server:

	• IPsec for communication with a Domain Controller for smart card authentication and with all remote print clients.
FTP_TRP.1(a)	The TOE enforces communications over HTTPS for a secure channel for administrators managing the TOE via the EWS interface. The communication channel is protected by the secure mechanisms of TLS. It 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(b)	The TOE uses IPsec to provide a trusted communications path for non-administrator TOE users sending print jobs from print clients. The TOE uses HTTPS/TLS when non-admin users access the WebUI' for scan jobs
FCS_HTTPS_EXT.1	HTTPS is implemented in the TOE according to RFC 2818, which specifies HTTP over TLS. The TOE acts as an HTTPS client when sending scanned images over HTTPS to a Workflow Repository file server. The TOE acts as an HTTPS Server for browser connections to the EWS.
FCS_TLS_EXT.1	The TOE implements TLS 1.2 for trusted channel communications. The TOE can be a client or server depending on the feature used. For EWS access, the TOE acts as a TLS server, client authentication is not supported. The TOE acts as a TLS client for communication with an LDAP authentication server (LDAPS), with a Mail Server (SMTP), and with a Workflow Repository file server (HTTPS). The following ciphersuites are supported: • *TLS_RSA_WITH_AES_128_CBC_SHA256* • *TLS_RSA_WITH_AES_256_CBC_SHA256* • *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256* • *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256* • *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256* • *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384* • *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256* • *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* • *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256* • *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384* • *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256* • *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
FCS_SSH_EXT.1	The TOE uses SSH/SFTP to transfer audit logs to a remote log server. Authentication to the SFTP server can be with username and password, or by way of private/public key pair

	as derived from certificates. Either of these methods is configurable at the TOE. The SSH transport supported algorithms are AES-CBC-128 and AES-CBC-256 only. Public key algorithm supported is SSH_RSA, ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384. The data integrity algorithms allowed in SSH transport connection are hmac-sha2-256, HMAC-SHA2-512. There is no configuration at the TOE to restrict or select any of the above protocols/algorithms other than username vs certificate. 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. Outgoing SFTP packets larger than 40,000 bytes are dropped. The TOE does not receive files over SFTP.
FCS_IPSEC_EXT.1	The TOE uses IPsec for communication with a Domain Controller for Smart Card authentication and to protect communication with all remote print clients. The TOE implements an IPsec Security Policy Database (SPD) and allows configuration to discard, bypass, and protect packets. 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. 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 desired evaluated configuration. The

	evaluated configuration is set up in order to test all possible actions of bypass, drop, and applied cryptography. Components of Policies (host/host group, protocol/protocol group, action): 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. 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. Action: Action of Protect: The following cryptographic protocols are supported: • Authentication Header (AH)–Allows authentication of the sender of data. • Encapsulating Security Payload (ESP)–Supports both sender authentication and data encryption. Both transport and tunnel mode are supported and are configuration options when configuring up IPsec. 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-SHA-256 and HMAC-SHA-384. 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. 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. 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 peer negotiations use RSA certificates along the DH mode configured (DH group 14), DH Group 19 (256-bit Random ECP), DH Group 20 (384-bit Random ECP), or via pre-shared keys.
FIA_PSK_EXT.1	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.

6.1.8 PSTN Fax-Network Separation

FDP_FXS_EXT.1	The only communication via the fax interface allowed is that of transmitting or receiving User Data using fax protocols. There is connection between the fax modem and the Ethernet or wireless interfaces. 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. 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. 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.

6.1.9 Data Clearing and Purging (Job Data Removal)

FDP_RIP.1(b)	The purge (also know as Job Data Removal) 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

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.

8. Glossary

For the purposes of this document, the following terms and definitions apply.

Access: Interaction between an entity and an object that results in the flow or modification of data.

Access Control: Security service that controls the use of hardware and software resources and the disclosure and modification of stored or communicated data.

Accountability: Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator: A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Asset: An entity upon which the TOE Owner, User, or manager of the TOE places value.

Authentication: Security measure that verifies a claimed identity.

Authentication data: Information used to verify a claimed identity.

Authorization: Permission, granted by an entity authorized to do so, to perform functions and access data.

Authorized User: An authenticated User who may, in accordance with the TSP, perform an operation, This includes Users who are permitted to perform some operations but may be able to attempt or perform operations that are beyond those permissions.

Availability: (A) A condition in which Authorized Users have access to information, functionality and associated assets when requested. (B) Timely (according to a defined metric), reliable access to IT resources.

Channel: Mechanisms through which data can be transferred into and out of the TOE.

Confidentiality: (A) A condition in which information is accessible only to those authorized to have access. (B) A security policy pertaining to disclosure of data.

Enterprise: An operational context typically consisting of centrally-managed networks of IT products protected from direct Internet access by firewalls. Enterprise environments generally include medium to large businesses, certain governmental agencies, and organizations requiring managed telecommuting systems and remote offices

Evaluation Assurance Level: An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

External Interface: A non-hardcopy interface where either the input is being received from outside the TOE or the output is delivered to a destination outside the TOE.

Function: an entity in the TOE that performs processing, storage, or transmission of data that may be present in the TOE.

Hardcopy Device (HCD): A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines,

digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones", and other similar products. See also: multifunction device.

Hardcopy Output Handler: Mechanisms for transferring User Document Data in hardcopy form out of the HCD.

Identity: A representation (e.g., a string) uniquely identifying an Authorized User, which can either be the full or abbreviated name of that User or a pseudonym.

Information assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Technology (IT): The hardware, firmware and software used as part of a system to collect, create, communicate, compute, disseminate, process, store or control data or information.

Integrity: (A) A condition in which data has not been changed or destroyed in an unauthorized way. (B) A security policy pertaining to the corruption of data and security function mechanisms.

Job: A document processing task submitted to the hardcopy device. A single processing task may process one or more documents.

Multifunction Device (MFD) and **Multifunction Product (MFP)**: A hardcopy device that fulfills multiple purposes by using multiple functions in different combinations to replace several, single function devices.

Nobody: A pseudo-role that cannot be assigned to any User.

Nonvolatile storage: Computer storage that is not cleared when the power is turned off.

Normal User: A User who is authorized to perform User Document Data processing functions of the TOE.

Object: A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operation: A specific type of action performed by a subject on an object.

Operational Environment: The total environment in which a TOE operates, including the consideration of the value of assets and controls for operational accountability, physical security and personnel.

Operator Panel: A local human interface used to operate the HCD. It typically consists of a keypad, keyboard, or other controls, and a display device.

Organizational Security Policy (OSP): A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Original Document Handler: Mechanisms for transferring User Document Data in hardcopy form into the HCD.

Own or **Ownership**: May refer to a User Document or to User Function Data associated with .processing a User Document. Depending upon the implementation of conforming TOE applications, the Owner of a User Function Data associated with a User Document may be different or may have different access control rules. These should be specified in a conforming Security Target.

Private-medium interface: Mechanism for exchanging data that (1) use wired or wireless electronic methods over a communications medium which, in conventional practice, is not accessed by multiple simultaneous users; or, (2) use Operator Panel and displays that are part of the TOE.

Protected: A condition in which data has not been changed or destroyed in an unauthorized way.

Removable nonvolatile storage: nonvolatile storage that is part of an evaluated TOE but is designed to be removed from the TOE by authorized personnel. See also Nonvolatile storage.

Security attribute: A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security Function Policy (SFP): A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.

Security Functional Requirement (SFR): A functional requirement which is taken from Part 2 of the Common Criteria and provide the mechanisms to enforce the security policy.

Security Target (ST): An implementation-dependent statement of security needs for a specific identified TOE.

SFR package: A named set of security functional requirements.

Shared-medium interface: Mechanism for transmitting or receiving data that uses wired or wireless network or non-network electronic methods over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users.

Subject: An active entity in the TOE that performs operations on objects.

Target of Evaluation (TOE): A set of software, firmware and/or hardware possibly accompanied by guidance.

Telephone line: An electrical interface used to connect the TOE to the public switch telephone network for transmitting and receiving facsimiles.

Threat: Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

TSF Data: Data created by and for the TOE, that might affect the operation of the TOE.

TSF Confidential Data: Assets for which either disclosure or alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE.

TSF Protected Data: Assets for which alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.

TOE Owner: A person or organizational entity responsible for protecting TOE assets and establishing related security policies.

TOE security functionality (TSF): A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

User: An entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User Data: Data created by and for the User, that do not affect the operation of the TOE security functionality.

User Document Data: The asset that consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually-stored data created by the hardcopy device while processing an original document and printed hardcopy output.

User Function Data: The asset that consists of the information about a user's document or job to be processed by the HCD.

9. Acronyms

For the purposes of this document, the following acronyms and definitions apply.

Table 18: Acronyms

Acronym	Definition
ALT	Alteration
B&W	Black and White
CAC	Common Access Card
CC	Common Criteria
CPY	Copy
CWIS	CenterWare Internet Services
DHCP	Dynamic Host Configuration Protocol
DIS	Disclosure
DSR	Document Storage And Retrieval
EAL	Evaluation Assurance Level
EIP	Extensible Interface Platform
EWS	Embedded Web Server
FIPS	Federal Information Processing Standard
HCD	Hardcopy Device
HCDPP	Protection Profile for Hardcopy Devices
HDD	Hard Disk Drive
I&A	Identification and Authentication
IEEE	Institute Of Electrical And Electronics Engineers
IIO	Immediate Image
IOT	Image Output Terminal
IPP	Internet Printing Protocol
IPsec	Internet Protocol Security
IT	Information Technology
LanFax	Enables fax jobs to be submitted from the desktop via printing protocols.
LDAP	Lightweight Directory Access Protocol
LPR	Line Printer Remote
LUI	Local User Interface
MFD	Multifunctional Device

Acronym	Definition
MFP	Multifunctional Product / Peripheral / Printer
NVM	Nonvolatile Memory
OSP	Organizational Security Policy
PIV	Personal Identity Verification
PPM	Page Per Minute
PP	Protection Profile
PRT	Print
PSTN	Public Switched Telephone Network
SCN	Scan
SFP	Security Function Policy
SFR	Security Functional Requirement
SMI	Shared-Medium Interface
SMTPS	Simple Mail Transfer Protocol Secure
SSD	Solid-State Drive
SSH	Secure Shell
ST	Security Target
Std	Standard
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
USB	Universal Serial Bus