Xerox® B410 Printer and C410 Color Printer Security Target with Firmware Version 222.037

Version 1.8
04 November 2024

Xerox Corporation
201 Merritt 7
Norwalk, CT 06851-1056
www.xerox.com

Prepared by:

Common Criteria Consulting, LLC
10346 Royal Woods Ct
Montgomery Village, MD 20886
www.consulting-cc.com

Revision History			
Date	Version	Author	Modifications
2023-09-22	0.1	CCC	Initial Draft. Base ST is Lexmark SFP ST v0.1.
2023-10-11	0.2	CCC	Added two mods to 6.1.3 TSS/Encryption to correct reference of User data to TSF data.
2023-10-12	0.3	CCC	Updated TOE ID from vxxxxx to with Firmware Version xxxxx.
2023-12-01	0.4	CCC	Addressed comments from Scheme.
2024-07-29	1.0	CCC	Addressed Errata.
2024-07-31	1.1	CCC	Updated firmware version.
2024-08-20	1.2	CCC	Updated TOE Documentation dates.
2024-08-20	1.3	CCC	Updated firmware to 222.037.
2024-10-08	1.4	CCC	Minor mods.
2024-10-11	1.5	CCC	Addressed ORs.
2024-10-17	1.6	CCC	Added FW to title page and removed /Rev.
2024-10-25	1.7	CCC	Addressed certifier ORs.
2024-11-04	1.8	CCC	Updated the company name.

Table of Contents

List of Figures and Tables

1. Security Target Introduction

1.1 Overview

This Security Target (ST) defines the Xerox B410 Printer and C410 Printer with Firmware Version 222.037 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

The Security Target (ST) contains the following sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

1.2 Security Target, Target of Evaluation, and Common Criteria Identification

ST Title: *Xerox® B410 Printer and C410 Color Printer Security Target with Firmware Version 222.037*

ST Version: 1.8

ST Date: 04 November 2024

Target of Evaluation (TOE) Identification: Xerox® B410 Printer and C410 Color Printer with Firmware Version 222.037.

TOE Developer: Xerox Corporation

Evaluation Sponsor: Xerox Corporation

CC Identification: *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, April 2017

1.3 Conformance Claims

The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5*. As such, the spelling of terms is presented using the internationally accepted English.

This ST and the TOE it describes claims exact conformance to the following CC specifications:

- *collaborative Protection Profile for Hardcopy Devices,* Version 1.0e, 4 March 2024 with the following conditionally mandatory, optional and selection based SFRs:
  - Conditionally Mandatory SFRs:
    - FCS_KYC_EXT.1 Extended: Key Chaining
    - FDP_DSK_EXT.1 Extended: Protection of Data on Disk
    - FIA_AFL.1 Authentication failure handling
    - FTP_KYP_EXT.1 Extended: Protection of Key and Key Material
    - FTP_TRP.1/NonAdmin Trusted path (for Non-Administrators)
  - Optional SFRs
    - FDP_UDU_EXT.1 Extended: Document Unavailability

    - FPT_WIPE_EXT.1 Data Wiping
  - Selection Based SFRs
    - FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)
    - FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
    - FCS_IPSEC_EXT.1 Extended: IPsec selected
    - FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
    - FIA_X509_EXT.1 X.509 Certificate Validation
    - FIA_X509_EXT.2 X.509 Certificate Authentication
    - FIA_X509_EXT.3 X.509 Certificate Requests

- *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.
  - Part 3 Conformant

1.4 Technical Decisions

All NIAP Technical Decisions issued to date and applicable to HCDcPP have been considered.

1.5 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.
  - Iteration: allows a component to be used more than once with varying operations. An iterated SFR is indicated by a slash followed by a descriptor for the purpose of the iteration. For example, FCS_HTTPS_EXT.1/Client indicates that the FCS_HTTPS_EXT.1 requirement applies specifically to HTTPS client functionality.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using italics and are surrounded by brackets (e.g., [*assignment item*]). Note that an assignment within a selection would be identified in both italics and underline, with the brackets themselves underlined since they are explicitly part of the selection text, unlike the brackets around the selection itself (e.g., [selection item, [*assignment item inside selection*]]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using underlines and are surrounded by brackets (e.g., [selection item]). Note that a selection within a selection would be identified underlined with the brackets themselves underlined since they are explicitly part of the selection text, unlike the brackets around the selection itself (e.g., [selection item, [selection inside selection]]).
  - Refinement: allows technical changes to a requirement to make it more restrictive and allows non-technical changes to grammar and formatting. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big**

things …"). Note that minor grammatical changes that do not involve the addition or removal of entire words (e.g., for consistency of quantity such as changing "meets" to "meet") do not have formatting applied.

- The ST does not retain the font formatting (bold, italicized, underlined text) of the HCDcPP.

1.5.1 Definitions

Table 1: Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
AD	Active Directory
AES	Advanced Encryption Standard
BSD	Berkeley Software Distribution
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CM	Configuration Management
CTR_DRBG	Counter Mode DRBG
DLE	Downloadable Emulators
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FAC	Function Access Control
FTP	File Transfer Protocol
GB	Gigabyte
GCM	Galois Counter Model
GSSAPI	Generic Security Services Application Program Interface
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
I&A	Identification & Authentication
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPP	Internet Printing Protocol
IPsec	Internet Protocol Security
ISO	International Standards Organization
IT	Information Technology
KAT	Known Answer Test
KDC	Key Distribution Center

Acronym/ Abbreviation	Definition
KMD	Key Management Description
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
NIAP	National Information Assurance Partnership
NAND	Not And
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OSP	Organizational Security Policy
PIV	Personal Identity Verification
PJL	Printer Job Language
P/N	Part Number
PP	Protection Profile
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
RBG	Random Bit Generator
RFC	Request For Comments
SFP	Security Function Policy
SFP	Single Function Printer
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SP	Special Publication
ST	Security Target
TD	Technical Decision
TOE	Target of Evaluation
TPM	Trusted Platform Module
TRNG	True Random Number Generator
TSF	TOE Security Function
UI	User Interface
USB	Universal Serial Bus

2. TOE Description

2.1 Type

This TOE is a digital Single Function Printer (SFP), which is an IT device that inputs, stores, and outputs electronic and hardcopy documents.

2.2 TOE Overview

The SFPs are single functional printer systems with network capabilities. Their capabilities extend to servicing print jobs through the network. The SFPs feature an integrated touch-sensitive operator panel.

The major security features of the TOE are:

1. All Users are identified and authenticated as well as authorized before being granted permission to perform any restricted TOE functions.
2. Administrators authorize Users to use the functions of the TOE.
3. User Document Data are protected from unauthorized disclosure or alteration.
4. TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.
5. TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.
6. Document processing and security-relevant system events are recorded, and such records are protected from disclosure to anyone except for authorized personnel. Records may not be altered.

The TOE includes two Xerox Single Function printers. Each of the SFPs in the TOE include a Trusted Platform Module (TPM) a standard printer component.

The Xerox printers are sold in predefined configurations, providing groupings of added options such as duplex printing and wireless communication. The configurations are identified by a character string appended to the model number. The following table provides details of the models and their configurations that are included in the evaluation.

Table 2: SFP TOE Configurations

Build	Models Included in the Evaluation	TPM
MSTSN	B410	Standard
CSTGV	C410	Standard

The firmware version of the TOE is *build*.222.037. Where *build* is one of the following:

- MXTSN for the B410 printers,
- CXTGV for the C410 printers,

The first letter in the build identifier is M for mono printers or C for color printers. The next two letters are always ST, signifying single function devices. The last two letters in the build identifier identify a specific processor used in the printer models.

2.2.1 Keywords

Hardcopy, Paper, Document, Printer, Document Server, Nonvolatile storage, Residual data, Temporary data, Network interface, Shared communications medium, SFP.

2.2.2 Physical Boundary

The physical boundary of the TOE is the software and hardware of the SFPs that include a standard TPM.

The functionality of all models is the same; the differences is limited to color support, paper sizes supported, and pages per minute the printers support. The following table provides the printer specifics.

Table 3: Technical Characteristics of the SFP Models

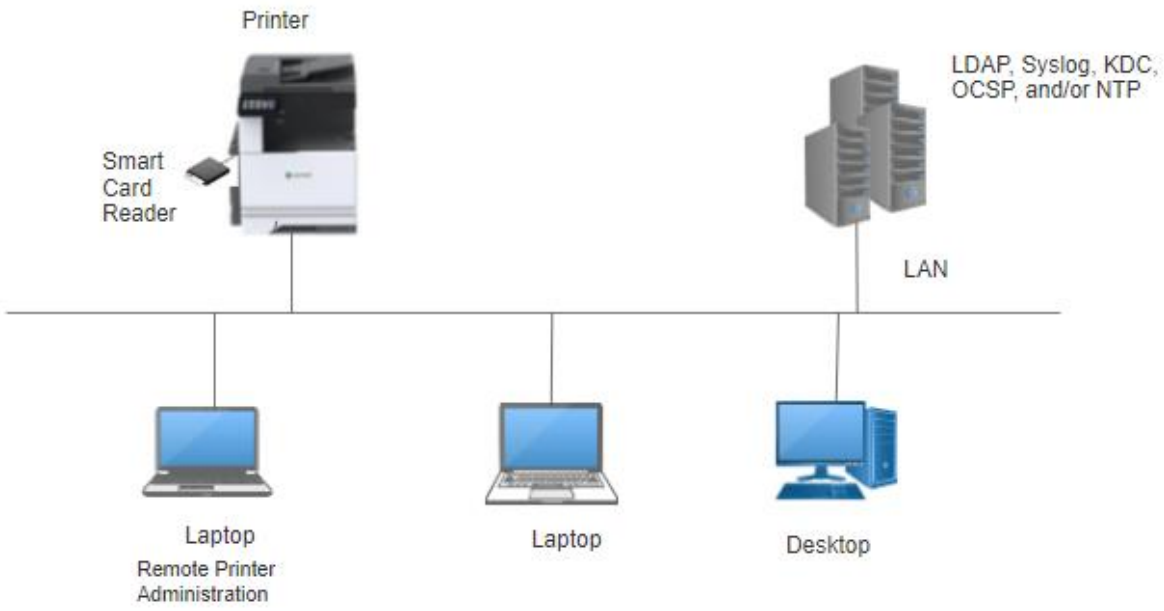
Model	Processor	Word Size	Color/Mono	Pages Per Minute
B410	Marvell 88PA6220 (Gem)	64-bit	Mono	50
C410	Marvell 88PA6220 (Gem)	64-bit	Color	42

The TPM included in the printers is an Infineon OPTIGA™ Trusted Platform Module SLB9672_2.0 version 15.21.16430.00. The TPM provides a DRBG that is used to supply entropy to the Xerox software DRBG. The TPM implements a NIST SP 800-90B CTR_DRBG and has been evaluated and included on CAVP certificate #A1582 and CMVP certificate #4347. Additionally, the TPM has been Common Criteria EAL4+ (AVA_VAN.4, ALC_FLR.1) certified (*Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0, v15.20.15686.00, v15.21.16430.00, v15.22.16832.00,* April 25, 2022).

Xerox uses reputable shipping firms that provide shipment tracking functionality to deliver printers. Delivery of the guidance docs via web site is addressed in ST section 2.2.3.9.

The following diagram depicts a representative TOE deployment.

Figure 1: Representative TOE Deployment



2.2.2.1 Required Non-TOE Hardware/Software/Firmware

To be fully operational, the following items may be connected to the SFP:

1. A LAN for network connectivity. The TOE supports IPv4 and IPv6.
2. An IT system acting as the remote syslog recipient of audit event records sent from the TOE.
3. IT systems that submit print jobs to the SFP via the network using standard print protocols.
4. An OCSP Server to verify the validity of X.509 certificates.
5. An IT system that connects remotely to the printer to perform remote configuration. Remote configuration is optional.
6. An LDAP Server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.
7. A card reader and cards to support Personal Identity Verification (PIV) cards. This component is optional depending on the type(s) of I&A mechanisms used. The supported card reader is the Identiv uTrust 2700 F Contact Smart Card Reader.
8. A Network Time Protocol Server. This system is optional based on if the time source is configured locally or remotely.

9. A Key Distribution Center (KDC). This system is optional and required only if smart card authentication is selected.

2.2.2.2 The Evaluated Configuration

2.2.2.2.1 Configuration of the Evaluated Configuration

The following configuration options apply to the evaluated configuration of the TOE. Refer to the *Xerox Common Criteria Installation Supplement and Administrator Guide* for guidance on configuration.

1. No optional network interfaces are installed on the SFPs. Note that one physical LAN interface is standard on all SFPs and must be used for the evaluated configuration. The wireless Ethernet connection needs to be disabled.
2. No optional parallel or serial interfaces are installed on the SFPs. These are for legacy connections to specific IT systems only.
3. No option card for downloadable emulators is installed in the TOE.
4. All USB ports on the SFPs that perform document processing functions (print) are disabled via configuration. If Smart Card authentication is used, the card reader is physically connected to a specific USB port during TOE installation; in the evaluated configuration this USB port is limited in functionality to acting as the interface to the card reader. A reader is shipped with the SFP. If Smart Card authentication is not used, the card reader may be left unconnected.
5. All unnecessary network ports are disabled.
6. Simple Network Management Protocol (SNMP) support is disabled.
7. No Java applications other than those stated in this section are loaded into the SFP by Administrators. These applications are referred to as eSF applications in the Xerox user documentation. If PIV smart card authentication is going to be used, the following eSF applications must be installed by an administrator during TOE installation and enabled: “Smart Card Authentication”, “Smart Card Authentication Client”, and “Background and Idle Screen”.
8. All other eSF applications installed by Xerox before the TOE is shipped must be disabled.
9. NPAP, PJL and Postscript have the ability to modify system settings. The capabilities specific to modifying system settings via these protocols are disabled.
10. All network communication is required to use IPSec with ESP to protect the confidentiality and integrity of the information exchanged, including management sessions that exchange D.TSF.CONF and D.TSF.PROT. Certificates presented by remote IT systems are validated.
11. The only supported Diffie-Hellman group for IKE is Group 14 (2048-bit MODP) and Group 15 (3072-bit MODP).
12. Operational management functions are performed via browser sessions to the embedded web server or via the management menus available through the touch panel.

13. I&A may use Username/Password Accounts and/or the LDAP+GSSAPI login method on a per-user basis. Smart Card authentication may be used for touch panel users. No other I&A mechanisms are included in the evaluation because they provide significantly lower strength than the supported mechanisms.
14. LDAP+GSSAPI and Smart Card authentication require integration with an external LDAP server such as Active Directory. This communication uses default certificates; the LDAP server must provide a valid certificate to the TOE. Binds to LDAP servers for LDAP+GSSAPI use device credentials (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific SFP. Binds to LDAP servers for Smart Card authentication use user credentials from the card (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific user.
15. Audit event records are transmitted to a remote IT system as they are generated using the syslog protocol. Because all network traffic is required to use IPSec with ESP, syslog records sent to a remote IT system also are protected by IPSec with ESP.
16. The severity level of audit events to log must be set to 5 (Notice).
17. Access controls are configured for all TSF data so that only authorized administrators are permitted to manage those parameters.
18. Configure Login failures parameter to a three or greater.
19. Administrators are directed (through operational guidance) to specify passwords adhering to the following composition rules for Username/Password Accounts:
    - A minimum of 8 characters (note that the minimum size is configurable and can be set to a minimum of 32 characters)
    - At least one lower case letter, one upper case letter, and one non-alphabetic character
    - No dictionary words or permutations of the username
20. All administrators must be authorized for all of the document processing functions (print).
21. The B/W Print and Color Print permissions must be configured for the Public permissions, which apply to all users including the Guest user. These permissions authorize the SFP to accept print jobs from remote IT systems. No other permissions may be configured for the Public permissions.
22. All network print jobs are held until released via the touch panel. Every network print job must include a PJL SET USERNAME statement to identify the userid of the owner of the print job. Held print jobs may only be released by an authenticated user with the same userid as specified in the print job.
23. The following parameters are disabled: Use Intelligent Storage Drive parameter; Internet Printing Protocol (IPP) support; Create Profiles; Remote Management; User Profiles
24. Create Profiles is disabled.

2.2.2.2.2 Evaluated Configuration Input/Destination

The following table defines the combinations of possible input sources and destinations that are included in the evaluated configuration. In the table, the following meanings are used:

- "May Be Disabled or Restricted" indicates that the functionality is included in the evaluation but may be disabled or restricted to an authorized set of users at the discretion of an administrator.
- "Disabled" indicates the functionality exists within the TOE but is always disabled by an administrator for the evaluated configuration.
- "n/a" indicates the functionality does not exist in the TOE.

Table 4: Source-Destination Combinations

Destination	Source
	Print Protocols (via the Network Interface)
Printer	Must be Enabled.
Outgoing Fax	n/a
Email (via the Network Interface)	n/a
FTP (via the Network Interface)	n/a

2.2.2.2.3 Functionality Excluded in the Evaluated Configuration

The following functionality is supported in the Xerox printers but is not included in the evaluation.

1. In addition to Personal Identity Verification (PIV) cards, Common Access Card (CAC) and Secret Internet Protocol Router Network (SIPRNet) cards are also supported.
2. In addition to the Identiv uTrust 2700 F Contact Smart Card Reader, the following card readers are also supported:
   a. Identiv uTrust 2700 R Contact Smart Card Reader,
   b. Omnikey 3121 SmartCard Reader,
   c. Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the Omnikey 3121 (example Omnikey 3021),
   d. SCM SCR 331,
   e. SCM SCR 3310v2.

2.2.3 Logical Boundary

This section summarizes the security functions provided by the TOE:

- Identification, Authentication and Authorization

- Access Control
- Encryption
- Trusted Communications
- Administrative Roles
- Auditing
- Trusted Operation
- Data Clearing and Purging

2.2.3.1 Identification, Authentication and Authorization

When a touch panel or web session is initiated, the user is implicitly assumed to be the Guest (default) user. Per the evaluated configuration, the permissions for this user must be configured such that no access to TSF data or functions is allowed other than print job submission (job submission is authorized regardless of what user is logged in). Therefore, the user must successfully log in as a different user before any TSF data or functions other than print job submission may be accessed.

The TOE supports I&A with a per-user selection of Username/Password Accounts (processed by the TOE) or integration with an external LDAP server (in the operational environment) using GSSAPI/Kerberos. Smart Card authentication may also be specified for users of the touch panel.

2.2.3.2 Access Control

Access controls configured for functions and menu access are enforced by the TOE.

2.2.3.3 Encryption

The TOE protects the confidentiality and integrity of all information exchanged over the attached network by using IPSec with ESP for all network communication.

2.2.3.4 Trusted Communications

The TOE ensures communication is performed with known endpoints by using IPSec with pre-shared keys or by validating supplied certificates.

2.2.3.5 Administrative Roles

Through web browser and touch panel sessions, authorized administrators may configure access controls and perform other TOE management functions.

2.2.3.6 Auditing

The TOE generates audit event records for security-relevant events. Audit records are stored internally and securely transmitted to a remote IT system using the syslog protocol over IPsec.

2.2.3.7 Trusted Operation

Software updates are verified to ensure the authenticity of the software before being applied. During initial start-up, the TOE performs self-tests on its cryptographic components and the integrity of the executable code.

2.2.3.8 Data Clearing and Purging

In the evaluated configuration, the TOE automatically overwrites memory containing printer information when the data is released.

2.2.3.9 TOE Documentation

Xerox provides the following product documentation in support of the installation and secure use of the TOE. The TOE guidance documentation shown below is available through the vendor's support portal and is available in .pdf format.

- Xerox® Common Criteria Installation Supplement and Administrator Guide, August 2024. Available upon request via submitting a Product Security Information Request.
- *Xerox B410 and C410 Printers Embedded Web Server Administrator Guide,* June 2023.
- *Xerox B410 Printer User Guide*, June 2023.
- *Xerox C410 Color Printer User Guide,* June 2023.

3. Security Problem Definition

This ST includes the Security Problem Definition, composed of threats, assumptions, and organizational security policies in the following sections.

In general, the threat model of the HCDcPP is designed to protect against the following:

- Disclosure of sensitive data at rest or in transit that the user has a reasonable expectation of security for.
- Excessive or poorly-implemented interfaces with the underlying platform that allow an application to be used as an intrusion point to a system.

This threat model is applicable to the TOE because data is transferred across the network and stored. It is also applicable because the TOE is a collection of executable binaries that an attacker could attempt to use to compromise the underlying OS platform if it was designed in such a manner that this exploitation was possible.

This Security Problem Definition is reproduced from Appendix I.1 through I.5 from the HCDcPP.

3.1 Users

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

Table 5: User Categories

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

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

3.2 Assets

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

Table 6: Asset Categories

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

There are no additional Asset categories defined in this ST.

3.2.1 User Data

User Data are composed of two types:

Table 7: User Data types

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

There are no additional User Data types defined in this ST.

3.2.2 TSF Data

TSF Data are composed of two types:

Table 8: TSF Data types

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

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

3.3 Threats

Threats are defined by a threat agent that performs an action resulting in an outcome that has the potential to violate TOE security policies.

Table 9: Threats

Designation	Definition

T.UNAUTHORIZED_AC CESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.
T.TSF_FAILURE	A malfunction of the TSF may compromise the device security status if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may install unauthorized firmware/software on the TOE to modify the Device security status.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.
T.WEAK_CRYPTO	An attacker may exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes to access (read, modify, or delete) TSF and User data.

3.4 Organizational Security Policies

Organizational Security Policies are used to provide a basis for Security Objectives that are not practical to define on the basis of Threats to Assets or that originate primarily from customer expectations.

Table 10: Organizational Security Policies

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

P.WIPE_DATA (optional)	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
P.ROT_INTEGRITY	The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters.

3.5 Assumptions

Assumptions are conditions that must be satisfied in order for the Security Objectives and functional requirements to be effective.

Table 11: Assumptions

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

4. Security Objectives

This ST includes the security objectives defined in the HCDcPP in the following sections. This includes security objectives for the TOE (used to mitigate threats) and for its operational environment (used to satisfy assumptions). The ST includes the two optional objectives O.IMAGE_OVERWRITE and O.WIPE_DATA.

The Security Objectives are reproduced from Appendix I.6 from the HCDcPP.

4.1 Security Objectives for the TOE

Table 12: Security Objectives for the TOE

Designation	Definition
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_AUTHORIZAT ION	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_VERIFICAT ION	The TOE shall provide mechanisms to verify the authenticity of firmware/software updates.
O.TSF_SELF_TEST	The TOE shall test some subset of its security functionality to help ensure that subset is operating properly.
O.COMMS_PROTECTI ON	The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.
O.AUDIT	The TOE shall generate audit data and store it internally as well as be capable of sending it to a trusted External IT Entity.
O.STORAGE_ENCRYPT ION	If the TOE stores User Document Data or Confidential TSF Data in Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices.
O.KEY_MATERIAL	The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material.

Designation	Definition
O.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Nonvolatile Storage Devices.
O.WIPE_DATA (optional)	The TOE provides a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
O.AUTH_FAILURES (conditionally mandatory)	The TOE resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.
O.FW_INTEGRITY	The TOE ensures its own integrity has remained intact and attests its integrity to outside parties on request.
O.STRONG_CRYPTO	The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards, including support for random bit generation based on recognized standards and a source of sufficient entropy. The TOE uses key sizes that are recognized as providing sufficient resistance to current attack capabilities.

4.2 Security Objectives for the Operational Environment

Table 13: Security Objectives for the Operational Environment

Designation	Definition
OE.PHYSICAL_PROTE CTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE.NETWORK_PROTE CTION	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 serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the following Protection Profile (PP):

- *collaborative Protection Profile for Hardcopy Devices*, Version 1.0e, 4 March 2024 (HCDcPP)

As a result, any selection, assignment, or refinement operations already performed by that PP on the claimed SFRs are not identified here (i.e., they are not formatted in accordance with the conventions specified in section 1.5 of this ST). Formatting conventions are only applied on SFR text that was chosen at the ST author's discretion.

5.1 Extended Requirements

All the extended requirements in this ST have been drawn from the HCDcPP. This document defines the extended SFRs; since they have not been redefined in this ST, the HCDcPP should be consulted for more information regarding these extensions to CC Parts 2 and 3.

- FAU_STG_EXT.1 Extended: External Audit Trail Storage
- FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
- FCS_IPSEC_EXT.1 Extended: IPsec selected
- FCS_KYC_EXT.1 Extended Key Chaining
- FCS_RBG_EXT.1 Extended Random Bit Generation
- FDP_DSK_EXT.1 Extended: Protection of Data on Disk
- FDP_UDU_EXT.1 Document Unavailability
- FIA_PMG_EXT.1 Extended: Password Management
- FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication
- FIA_X509_EXT.3 X.509 Certificate Requests
- FPT_KYP_EXT.1 Extended: Protection of Key and Key Material
- FPT_SBT_EXT.1 Extended: Secure Boot
- FPT_SKP_EXT.1 Extended: Protection of TSF Data
- FPT_TST_EXT.1 Extended: TSF testing
- FPT_TUD_EXT.1 Extended: Trusted Update
- FPT_WIPE_EXT.1 Data Wiping

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE.

Table 14: TOE Security Functional Components

Requirement Class	Requirement Component
Security Audit (FAU)	FAU_GEN.1 Audit data generation

	FAU_GEN.2 User identity association
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_STG.1 Protected audit trail storage
	FAU_STG.4 Prevention of audit data loss
	FAU_STG_EXT.1 Extended: External Audit Trail Storage
Cryptographic Support (FCS)	FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric Keys)
	FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys)
	FCS_CKM.2 Cryptographic Key Establishment
	FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)
	FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)
	FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
	FCS_IPSEC_EXT.1 Extended: IPsec selected
	FCS_KYC_EXT.1 Extended: Key Chaining
	FCS_RBG_EXT.1 Extended: Random Bit Generation
User Data Protection (FDP)	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
	FDP_DSK_EXT.1 Extended: Protection of Data on Disk
	FDP_UDU_EXT.1 Document Unavailability
Identification and Authentication (FIA)	FIA_AFL.1 Authentication failure handling
	FIA_ATD.1 User attribute definition
	FIA_PMG_EXT.1 Extended: Password Management
	FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
	FIA_UAU.1 Timing of authentication
	FIA_UAU.7 Protected authentication feedback
	FIA_UID.1 Timing of identification
	FIA_USB.1 User-subject binding

	FIA_X509_EXT.1 X.509 Certificate Validation
	FIA_X509_EXT.2 X.509 Certificate Authentication
	FIA_X509_EXT.3 X.509 Certificate Requests
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Privacy (FPR)	There are no class FPR requirements.
Protection of the TSF (FPT)	FPT_KYP_EXT.1 Extended: Protection of Key and Key Material
	FPT_SBT_EXT.1 Extended: Secure Boot
	FPT_SKP_EXT.1 Extended: Protection of TSF Data
	FPT_STM.1 Reliable time stamps
	FPT_TST_EXT.1 Extended: TSF testing
	FPT_TUD_EXT.1 Extended: Trusted Update
	FPT_WIPE_EXT.1 Data Wiping
Resource Utilization (FRU)	There are no class FRU requirements.
TOE Access (FTA)	FTA_SSL.3 TSF-initiated termination
Trusted Paths/Channels (FTP)	FTP_ITC.1 Inter-TSF trusted channel
	FTP_TRP.1/Admin Trusted path (for Administrators)
	FTP_TRP.1/NonAdmin Trusted path (for Non-Administrators)

5.2.1 Security Audit (FAU)

5.2.1.1 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 **15**, [*no other auditable events*].

Refinement Rationale: The table reference is changed to reflect the contents of the ST.

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 **15**, [*no other information*].

Refinement Rationale: The table reference is changed to reflect the contents of the ST.

Table 15: Auditable Events

Auditable Event	Relevant SFR	Additional Information
Job Completion	FDP_ACF.1	Type of Job
Unsuccessful login attempts limit is met or exceeded	FIA_AFL.1	None
Unsuccessful User authentication	FIA_UAU.1	Supplied User ID/Name and origin of the attempt (e.g., IP address)
Unsuccessful User identification	FIA_UID.1	Supplied User ID/Name and origin of the attempt (e.g., IP address)
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1/Admin, FTP_TRP.1/NonAdmin	Reason for failure
Unsuccessful attempt to validate a certificate	FIA_X509_EXT.1	Reason for failure of certificate validation

5.2.1.2 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.

5.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [an Administrator] with the capability to read [all records] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.4 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.2.1.5 FAU_STG.1 Protected audit trail storage

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

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

5.2.1.6 FAU_STG.4 Prevention of audit data loss

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

5.2.1.7 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.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric Keys)

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

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

].

5.2.2.2 FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys)

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

5.2.2.3 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

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

- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].

].

5.2.2.4 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.

5.2.2.5 FCS_CKM.4 Cryptographic key destruction

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

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

] that meets the following: [no standard].

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

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

- AES used in [CBC] mode,

] and cryptographic key sizes [

Case: AES algorithm [

[

- 256 bits],

] that meet the following [

Case: AES algorithm

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

].

5.2.2.7 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash Refinement: The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [

- SHA-256,
- SHA-384

] and message digest sizes [

- 256,
- 384

] bits that meet the following: [ISO/IEC 10118-3:2004].

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

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

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

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

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits, 3072 bits*]

] that meet the following: [

Case: RSA schemes

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

].

5.2.2.10 FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)

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

- AES used in [CBC] mode

] and cryptographic key sizes [

Case: AES algorithm

- [256 bits],

] that meet the following [

Case: AES algorithm

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

].

5.2.2.11 FCS_IPSEC_EXT.1 Extended: IPsec selected

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

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

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

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [AES-CBC-256 (RFC 3602)] together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA- 256, HMAC-SHA-384].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [RFC 4304 for extended sequence numbers], and [no other RFCs for hash functions];
- IKEv2 as defined in RFC 5996 and [with no support for NAT traversal], and [no other RFCs for hash functions]

].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1, IKEv2] protocol uses the cryptographic algorithms [AES-CBC-256 (specified in RFC 3602].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on [
  - length of time, where the time values can be configured within [*1-24*] hours;];
- IKEv2 SA lifetimes can be configured by a Security Administrator based on [
  - length of time, where the time values can be configured within [*1-24*] hours]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on [
  - length of time, where the time values can be configured within [*1-8*] hours;];
- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [
  - length of time, where the time values can be configured within [*1-8*] hours;]

].

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

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv1, IKEv2] exchanges of length [

- according to the security strength associated with the negotiated Diffie-Hellman group
- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash;

].

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

- [14 (2048-bit MODP), 15 (3072-bit MODP)] according to RFC 3526

].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 1, IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2, IKEv2 CHILD_SA] connection.

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

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

5.2.2.12 FCS_KYC_EXT.1 Extended: Key Chaining

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [one] while maintaining an effective strength of [256 bits].

5.2.2.13 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG ([AES])].

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

5.2.3 User Data Protection (FDP)

5.2.3.1 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 **16** and Table **17**.

Refinement Rationale: The table reference is changed to reflect the contents of the ST.

5.2.3.2 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 **16** and Table **17**.

Refinement Rationale: The table reference is changed to reflect the contents of the ST.

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 **16** and Table **17**].

Refinement Rationale: The table reference is changed to reflect the contents of the ST.

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: [

- *The Job Owner of submitted print jobs is determined by a Userid included in the embedded PJL. Print jobs received without a Userid, or with an unknown Userid, or with a Userid of a user that does not have the Held Jobs Access permission, are deleted after the specified timeout period for releasing held print jobs. During this time, no access to the print jobs is possible since access is restricted to the job owner.*

].

Table 16: D.USER.DOC Access Control SFP

PRINT	"Create"	"Read"	"Modify"	"Delete"
Operation:	Submit a document to be printed	View image or Release printed output	Modify stored document	Delete stored document
Job owner (with Held Jobs Access)	Yes	Release	No	Yes
Job owner (without Held Jobs Access)	Yes, but deleted	denied	denied	denied
Unknown user	Yes, but deleted	denied	denied	denied
No userid specified	Yes, but deleted	denied	denied	denied
U.ADMIN	U.ADMIN has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above.			
U.NORMAL	U.NORMAL has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above.			
Unauthenticated	See above categories	denied	denied	denied
SCAN	"Create"	"Read"	"Modify"	"Delete"
Operation:	Submit a document for scanning	View scanned image	Modify stored document	Delete stored document

Job owner (with E-mail Function permission)	n/a	n/a	n/a	n/a
U.ADMIN	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a
COPY	"Create"	"Read"	"Modify"	"Delete"
Operation:	Submit a document for copying	View scanned image or Release printed copy output	Modify stored document	Delete stored document
Job owner (with Copy Function permission)	n/a	n/a	n/a	n/a
U.ADMIN	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a
FAX SEND	"Create"	"Read"	"Modify"	"Delete"
Operation:	Submit a document to send as a fax	View scanned image	Modify stored document	Delete stored document
Job owner (with Fax Function permission)	n/a	n/a	n/a	n/a
U.ADMIN	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a
FAX RECEIVE	"Create"	"Read"	"Modify"	"Delete"
Operation:	Receive a fax and store it	View fax image or Release printed fax output	Modify image of received fax	Delete image of received fax
Fax owner (U.ADMIN with Release Held Faxes)	n/a	n/a	n/a	n/a
U.ADMIN (without Release Held Faxes)	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a
STORAGE/RETRIEVAL	"Create"	"Read"	"Modify"	"Delete"
Operation:	Store document	Retrieve stored document	Modify stored document	Delete stored document
Job owner	n/a	n/a	n/a	n/a
U.ADMIN (without Release Held Faxes)	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a

Unauthenticated	n/a	n/a	n/a	n/a

Table 17: D.USER.JOB Access Control SFP

PRINT	"Create"*	"Read"	"Modify"	"Delete"
Operation:	Create a print job	View print queue / job	Modify print job	Cancel print job
Job owner (with Held Jobs Access)	Yes	Yes, for itself	Modify # of copies	Yes, for itself
Job owner (without Held Jobs Access)	Yes, but deleted	denied	denied	denied
Unknown user	Yes, but deleted	denied	denied	denied
No userid specified	Yes, but deleted	denied	denied	denied
U.ADMIN	U.ADMIN has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above.			
U.NORMAL	U.NORMAL has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above.			
Unauthenticated	See above categories	denied	denied	denied
SCAN	"Create"	"Read"	"Modify"	"Delete"
Operation:	Create scan job	View scan status / log	Modify scan job	Cancel scan job
Job owner (with E-mail Function permission)	n/a	n/a	n/a	n/a
U.ADMIN	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a
COPY	"Create"	"Read"	"Modify"	"Delete"
Operation:	Create copy job	View copy status / log	Modify copy job	Cancel copy job
Job owner (with Copy Function permission)	n/a	n/a	n/a	n/a
U.ADMIN	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a
FAX SEND	"Create"	"Read"	"Modify"	"Delete"
Operation:	Create fax send job	View fax job queue / log	Modify fax send job	Cancel fax send job
Job owner (with Fax Function permission)	n/a	n/a	n/a	n/a
U.ADMIN	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a

FAX RECEIVE	"Create"	"Read"	"Modify"	"Delete"
Operation:	Create fax receive job	View fax receive status / log	Modify fax receive job	Cancel fax receive job
Fax owner (U.ADMIN with Release Held Faxes)	n/a	n/a	n/a	n/a
U.ADMIN (without Release Held Faxes)	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a
STORAGE/RETRIEVAL	"Create"	"Read"	"Modify"	"Delete"
Operation:	Create storage / retrieval job	View storage / retrieval log	Modify storage / retrieval job	Cancel storage / retrieval job
Job owner	n/a	n/a	n/a	n/a
U.ADMIN	n/a	n/a	n/a	n/a
U.NORMAL	n/a	n/a	n/a	n/a
Unauthenticated	n/a	n/a	n/a	n/a

5.2.3.3 FDP_DSK_EXT.1 Extended: Protection of Data on Disk

FDP_DSK_EXT.1.1 The TSF shall [perform encryption in accordance with FCS_COP.1/StorageEncryption], such that any Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext Confidential TSF Data.

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

5.2.3.4 FDP_UDU_EXT.1 Document Unavailability

FDP_UDU_EXT.1.1 The TSF shall ensure that any previous information content stored on a [non-wear-leveled storage device] of a resource is made unavailable [by overwriting data] upon the deallocation of the resource from the following objects: D.USER.DOC.

5.2.4 Identification and Authentication (FIA)

5.2.4.1 FIA_AFL.1 Authentication failure handling

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the account for an administrative configurable amount of time*].

5.2.4.2 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*
- *Associated groups*
- *User permissions, as specified by associated groups,*
- *Number of consecutive authentication failures,*
- *Time of the earliest authentication failure (since the last successful login if any have occurred),*
- *Account lock status*

].

5.2.4.3 FIA_PMG_EXT.1 Extended: Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")", *[other ASCII characters except CR and NL]*];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater.

5.2.4.4 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 256 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 [*[a pseudo-random function (PRF) using HMAC-SHA2-256 or HMAC-SHA2-384]*] and be able to [use no other pre-shared keys].

5.2.4.5 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 Refinement: The TSF shall allow [

- *submit print jobs;*
- *view operational status of the device,*

] 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.

5.2.4.6 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [*only asterisks ("*") or dots ("•")*] to the user while the authentication is in progress.

Application Note: asterisks are displayed for smart card users and dots are displayed for a touch screen user.

5.2.4.7 FIA_UID.1 Timing of identification

FIA_UID.1.1 Refinement: The TSF shall allow [

- *submit print jobs;*
- *view operational status of the device,*

] 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.

5.2.4.8 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*
- *Associated groups*
- *User permissions*

].

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: [

- *The username are the values supplied by the user.*
- *The associated groups are the values configured for the user account.*
- *User permissions are determined by combining the configured permissions for each associated group*.

].

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: [*the security attributes do not change during a session*].

5.2.4.9 FIA_X509_EXT.1 X.509 Certificate Validation

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

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

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

5.2.4.10 FIA_X509_EXT.2 X.509 Certificate Authentication

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

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

5.2.4.11 FIA_X509_EXT.3 X.509 Certificate Requests

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

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

5.2.5 Security Management (FMT)

5.2.5.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [

- *Audit*
- *Identification and authentication*
- *Authorization and access controls*
- *Communication with External IT Entities*
- *Network communications*
- *System or network time source*
- *Device functions (e.g., printing)*

] to [U.ADMIN].

5.2.5.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 Refinement: The TSF shall enforce the [User Data Access Control SFP] to restrict the ability to [

- query,
- modify,
- delete,
- *[create]*

] the security attributes [

- *Username,*
- *associated groups,*
- *user permissions*

] to [*administrators authorized for access to the Security Menu*].

5.2.5.3 FMT_MSA.3 Static attribute initialization

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

FMT_MSA.3.2 Refinement: The TSF shall allow the [no role] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.4 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 **18**.

Refinement Rationale: The table reference is changed to reflect the contents of the ST.

Table 18: Management of the TSF

Data	Operation	Authorized role(s) (for the user's own jobs only)
TSF Data owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL		
D.USER.JOB	Query, Modify	**Held Jobs Access (for the user's own jobs only)**
TSF Data not owned by a U.NORMAL		
Active Directory Configuration	*Create*	**Security Menu**
Date and Time Parameters	Query, Modify	**Device Menu**
Enable Audit	Query, Modify	**Security Menu**
Enable HTTP Server	Query, Modify	**Network/Ports Menu**
Enable Remote Syslog	Query, Modify	**Security Menu**
Groups	Query, Modify, Delete, Create	**Security Menu**
Held Print Job Expiration Timer	Query, Modify	**Security Menu**
IPSec Settings	Query, Modify	**Network/Ports Menu**
Job Waiting	Query, Modify	**Device Menu**
Kerberos Setup	Query, Modify	**Security Menu**
LDAP Certificate Verification	Query, Modify	**Security Menu**
LDAP+GSSAPI – SFP Credentials	Query, Modify	**Security Menu**
LDAP+GSSAPI Configuration	Query, Modify, Delete, Create	**Security Menu**
Login Restrictions	Query, Modify	**Security Menu**
Network Port	Query, Modify	**Security Menu**
Permissions	Query, Modify	**Security Menu**
Remote Syslog Parameters	Query, Modify	**Security Menu**
Security Reset Jumper	Query, Modify	**Security Menu**
Smart Card Authentication Client Configuration	Query, Modify	**Security Menu**

Data	Operation	Authorized role(s) (for the user's own jobs only)
USB Buffer	Query, Modify	**Network/Ports Menu**
Username/Password Accounts	Query, Modify, Delete, Create	**Security Menu**
Visible Home Screen Icons	Query, Modify	**Device Menu**
Software, firmware, and related configuration data		
Firmware	Query	**Reports Menu**
	Modify	**Firmware Updates**

5.2.5.5 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [

- *User management (e.g., add/change/remove local user)*
- *Role management (e.g., assign/deassign role relationship with user)*
- *Configuring identification and authentication (e.g., selecting between local and external I&A)*
- *Configuring authorization and access controls (e.g., access control lists for TOE resources)*
- *Configuring communication with External IT Entities*
- *Configuring network communications*
- *Configuring the system or network time source*
- *Configuring data transmission to audit server*
- *Configuring internal audit log storage*
- *Configure applications*
- *Perform firmware updates*
- *Configure device functions*
- *Sanitize device.*

].

5.2.5.6 FMT_SMR.1 Security roles

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

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

5.2.6 Privacy (FPR)

There are no class FPR requirements.

5.2.7 Protection of the TSF (FPT)

5.2.7.1 FPT_KYP_EXT.1 Extended: Protection of Key and Key Material (cm)

FPT_KYP_EXT.1.1 The TSF shall [

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

  ]

].

5.2.7.2 FPT_SBT_EXT.1 Extended: Secure Boot

FPT_SBT_EXT.1.1 The TSF shall contain one or more chains of trust with each chain of trust anchored in a Root of Trust that is implemented in immutable code or a HW-based write-protection mechanism.

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

FPT_SBT_EXT.1.3 The TSF shall [halt boot process] in the event of a boot time verification failure so that the corrupted firmware/software isn't executed.

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

FPT_SBT_EXT.1.5 The TSF shall contain [hash data] in the Hardware Root of Trust.

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

5.2.7.3 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.

5.2.7.4 FPT_STM.1 Reliable time stamps

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

5.2.7.5 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.

5.2.7.6 FPT_TUD_EXT.1 Extended: Trusted Update

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

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

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

5.2.7.7 FPT_WIPE_EXT.1 Data Wiping

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

- logically addresses the storage location of the data and performs a [single] overwrite consisting of [ones]

] that meets the following: [no standard].

5.2.8 Resource Utilization (FRU)

There are no class FRU requirements.

5.2.9 TOE Access (FTA)

5.2.9.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*configurable time interval of user inactivity in the range of 1 to 120 minutes for the web interface and 10 to 300 seconds for the touch panel*].

5.2.10 Trusted Paths/Channels (FTP)

5.2.10.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall use [IPsec] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: remote audit server, [authentication server, *[network time 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.

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

FTP_ITC.1.2 Refinement: The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 Refinement: The TSF shall initiate communication via the trusted channel for remote audit, [*remote authentication, network time synchronization*].

5.2.10.2 FTP_TRP.1/Admin Trusted path (for Administrators)

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

FTP_TRP.1.2/Admin Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

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

5.2.10.3 FTP_TRP.1/NonAdmin Trusted path (for Non-Administrators) (cm)

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

FTP_TRP.1.2/NonAdmin Refinement: The TSF shall permit [the TSF, remote users] to initiate communication via the trusted path

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

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference to the HCDcPP.

Table 19: Assurance Components

Assurance Class	Assurance Component
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)

Assurance Class	Assurance Component
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – conformance (ATE_IND.1)
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.1)

6. TOE Summary Specification

This chapter describes the following security functions:

- Identification, Authentication and Authorization
- Access Control
- Encryption
- Trusted Communications
- Administrative Roles
- Auditing
- Trusted Operation
- Data Clearing and Purging

6.1 Security Functions

6.1.1 Identification, Authentication and Authorization

Users are required to successfully complete the I&A process before they are permitted to access any restricted data or functionality. The set of restricted user functionality is under the control of the administrators, with the exception of submission of network print jobs which is always allowed.

A new session is established for the touch panel when the system boots and for web sessions when the connection is established. All sessions are initially bound to the Guest (default) user. In the evaluated configuration, the Guest user has no access to restricted functions or data other than allowing print jobs to be submitted.

Users must log in as a different user in order to gain access to TOE functionality. Multiple login mechanisms are supported in the evaluated configuration: Smart Card authentication, Username/Password Accounts and LDAP+GSSAPI. Note that Smart Card and LDAP+GSSAPI authentications also use Kerberos functionality when authenticating certificates or credentials. Username/Password information is stored in flash.

For Smart Card authentication, no functions at the touch panel are allowed until I&A successfully completes. The touch panel displays a message directing the user to insert a card into the attached reader. Once a card is inserted, the user is prompted for a PIN. When the PIN is entered, only asterisks ("*") are displayed. Once the PIN is collected (indicated by the user touching the Next button), the TOE passes the PIN to the card for validation. If it is not valid, a message is displayed on the touch panel and the user is asked to re-enter the PIN. After the card-configured number of consecutive invalid PINs, the card will lock itself until unlocked by a card administrator.

Upon successful card validation, the TOE forwards the certificate from the card to the configured Kerberos Key Distribution Center (KDC) (Windows Domain Controller) for validation. If the certificate validation is not successful, an error message is displayed on the touch panel until the current card is removed from the reader. If the certificate validation is successful, the TOE binds the username, account name, and email

address (all obtained from the KDC/LDAP server) to the user session for future use. An audit record for the successful authentication is generated. All communication with the KDC and LDAP server uses IPsec.

For Username/Password Accounts and LDAP+GSSAPI, the TOE collects a username and password via the touch panel or via the browser session. When the password is entered, only asterisks ("*") or dots ("●") are displayed. Asterisks are displayed on the touch panel; dots are displayed on the web interface. Once the username and password are collected, the next step in the process depends on the I&A mechanism being used.

For Username/Password Accounts, the TOE performs the validation of the username and password against the set of configured Username/Password Accounts. If the validation fails because of an invalid password (for a valid username), the count of failed authentication attempts is incremented for that account. If the threshold for failed attempts within a time period is reached, then the account is marked as being locked for the configured amount of time to mitigate against brute force password attacks.

For LDAP+GSSAPI, the TOE hashes the supplied password and forwards the username in an authentication request signed by the hashed password to the configured KDC for validation (using the configured machine credentials) and waits for the response. If no response is received, the validation is considered to have failed.

In the case of failed validations, an error message is displayed via the touch panel or browser session, and then the display returns to the previous screen for further user action. An audit record for the failed authentication attempt is generated.

If validation is successful, the TOE retrieves the account name and email address from the LDAP server and binds them to the user session for future use. An audit record for the successful authentication is generated.

Permissions for the user session are determined from group memberships. Authorized Administrators assign roles to user accounts by configuring permissions for each configured group and then assigning user accounts to groups. At minimum, during installation Authorized Administrators must perform the user account configuration activities in the guidance documentation to establish the evaluated configuration:

- Create new groups for Authorized Administrators and Authorized Users. The group names must correspond to names used in the LDAP server of Smart Card or LDAP+GSSAPI authentication is used.
- Configure appropriate permissions for each of those groups
- Assign all users and administrators using Username/Password Accounts to groups
- Modify the Public permissions (which are the only permissions for the Guest user account so that only B/W Print and Color Print are configured

For Username/Password accounts, the permissions for each group that the user is a member of (as specified in the account configuration) are combined. For Smart Cards and LDAP+GSSAPI, a list of group memberships are retrieved from the LDAP server. For each of those groups that match a group configured

in the TOE, the permissions are combined. If the group memberships or permissions are changed, active sessions are not affected; the changes take effect at the next login.

The user session is considered to be active until the user explicitly logs off, removes the card or the administrator-configured inactivity timer for sessions expires. The timer values are separately configurable: 1 to 120 minutes for the web interface and 10 to 300 seconds for the touch panel.

Users of the TOE, whether accessing the TOE via the touch panel or web interface, are considered to be in one or more of the following categories:

- Authorized Users – permitted to perform one or more of the user functions defined in FDP_ACC.1 and FDP_ACF.1.
- Authorized Administrators – permitted to access administrative functionality for control and monitoring of the SFP operation.
- Any Users – Authorized Users and Authorized Administrators

The following Permissions may be configured for groups:

Table 20: Permissions

Item	Description	Comment
Address Book	Controls the ability to manage the Address Book contents.	Permission may only be granted to authorized administrators in the evaluated configuration
Apps Configuration	Controls access to the configuration of any installed applications	Permission may only be granted to authorized administrators in the evaluated configuration.
B/W Print	Controls the ability to accept black and white print jobs.	Permission must be granted to the Public permissions
Cancel Jobs at the device	Controls access to the functionality to cancel jobs via the touch panel.	Permission may only be granted to authorized users in the evaluated configuration
Change Language from Home Screen	Controls access to the Change Language button on the Home screen (when displayed); this button is NOT displayed by default, but a user can activate it via the "General Settings Menu"	Permission may be granted to any users
Color Dropout	Controls a user's ability to activate the Color Dropout functionality as part of a job; if protected and the user fails to authenticate, then the	Permission may only be granted to authorized users in the evaluated configuration

Item	Description	Comment
	device DOES NOT use the color dropout functionality in the job	
Color Print	Controls the ability to print color jobs.	Permission must be granted to the Public permissions
Device Menu	Controls access to the Device administrative menu	Permission may only be granted to authorized administrators in the evaluated configuration
Firmware Updates	Controls a user's ability to update the device's firmware code via the network	Permission may only be granted to authorized administrators in the evaluated configuration
Flash Drive Color Printing	Controls whether USB interfaces may be used for color print operations	Permission must not be specified for any user
Flash Drive Print	Controls whether USB interfaces may be used for black and white print operations	Permission must not be specified for any user
Flash Drive Scan	Controls whether USB interfaces may be used for scan operations	Permission must not be specified for any user
FTP Function	Controls a user's ability to access the FTP button on the Home Screen (when displayed).	Permission must not be specified for any user
Function Configuration Menus	Controls access to the configuration menus for the print.	Permission may only be granted to authorized administrators in the evaluated configuration
Held Jobs Access	Controls access to the Held Jobs function	Permission may only be granted to authorized users in the evaluated configuration
Import/Export Settings	Controls the ability to import and export configuration files	Permission may only be granted to authorized administrators in the evaluated configuration
Internet Printing Protocol (IPP)	Controls access to print job submission via IPP	Permission must not be specified for any user
Manage Bookmarks	Controls access to the Delete Bookmark, Create Bookmark, and Create Folder buttons from both the bookmark list screen and from the individual bookmark screen	Permission must not be specified for any user

Item	Description	Comment
Manage Shortcuts	Controls access to the Manage Shortcuts Menu	Permission must not be specified for any user
Network/Ports Menu	Controls access to the Network/ Ports Menu	Permission may only be granted to authorized administrators in the evaluated configuration
New Apps	Controls access to configuration parameters for apps subsequently added to the device.	Permission may only be granted to authorized administrators in the evaluated configuration
Operator Panel Lock	Controls access to the "Lock Device" and "Unlock Device" buttons	Permission may only be granted to authorized users in the evaluated configuration
Option Card Menu	Controls a user's ability to access the "Option Card Menu" that displays menu nodes associated with installed DLEs	Permission may only be granted to authorized administrators in the evaluated configuration
Out of Service Erase	Controls the ability to wipe the storage of the SFP when it is being taken out of service.	Permission may only be granted to authorized administrators in the evaluated configuration
Paper Menu	Controls access to the Paper Menu	Permission may be granted to any users
Remote Management	Controls whether or not management functions may be invoked from remote IT systems	Permission must not be specified for any user
Reports Menu	Controls access to the Reports Menu. This includes information about user jobs, which can't be disclosed to non-administrators.	Permission may only be granted to authorized administrators in the evaluated configuration
Security Menus	Controls access to the Security Menu	Permission may only be granted to authorized administrators in the evaluated configuration
Supplies Menus	Controls access to the Security Menu	Permission may only be granted to authorized administrators in the evaluated configuration
Use Profiles	Controls a user's ability to execute any profile	Permission must not be specified for any user

The following SFRs satisfy Identification, Authentication, and Authorization.

FCS_CKM_EXT.4	When Username/Password accounts are deleted, the associated password is destroyed in flash.
FIA_AFL.1	Consecutive login failures for each user account within a configured time period are tracked, and if the configured limit is reached the user account is automatically locked for the configured amount of time.
FIA_ATD.1	The TSF maintains the following security attributes for users: • Username (configured for internal account, acquired from LDAP server AD and Smartcards) • Password (internal accounts) • Associated groups (configured for internal account, acquired from LDAP server AD and Smartcards) • Permissions (dynamically determined by group memberships) • Number of consecutive login failures • Time of earliest login failure (since last successful login) • Account lock status
FIA_PMG_EXT.1	Passwords for internal accounts are configured by administrators. The minimum password length is configurable from 1-32 characters. Passwords may contain any ASCII characters other than NL and CR.
FIA_UAU.1	User interaction through the touch panel and web interface prior to successful authentication is limited to viewing the operational status of the device (e.g., low paper). Users may submit print jobs without authenticating, but the jobs are not printed until released by the authenticated user.
FIA_UAU.7	When a password or PIN is entered for authentication, only asterisks ("*") or dots ("●") are displayed.
FIA_UID.1	User interaction through the touch panel and web interface prior to successful identification is limited to viewing the operational status of the device. Users may submit print jobs and supply identification via embedded PJL, but the jobs are not printed until released by the authenticated user. Invalid and missing identification in print jobs results in those print jobs being deleted.
FIA_USB.1	Upon successful login, the username, associated groups and permissions are bound to the session. The username is the value specified during login or the username associated with the certificate from a smartcard. The groups are those configured internally or on the LDAP server. The permissions are the union of the permissions for each associated group. These bindings do not change during an active session.

FTA_SSL.3	Upon expiration of an inactivity timer, the corresponding session is automatically terminated.

6.1.1.1 Active Directory Additional Information

If Active Directory parameters are supplied and Join is selected, the parameter values are used to join the Active Directory Domain. If successful, machine credentials are generated and the LDAP+GSSAPI configuration parameters are automatically updated with the Domain and machine information.

Once the Domain has been joined, subsequent I&A attempts may use the LDAP+GSSAPI configuration to validate user credentials using the newly-created machine credentials as described above. The credentials specified for Active Directory by an authorized administrator are not saved.

Communication with the Active Directory server uses IPsec.

6.1.2 Access Control

Access control validates a user access request against the session's permissions.

Authorization is restricted by not associating a permission with a function.

When the FAC is a menu, access is also restricted to all submenus (a menu that is normally reached by navigating through the listed item). This is necessary for instances where a shortcut could bypass the listed menu. If a shortcut is used to access a sub-menu, the access control check for the applicable menu item is still performed (as if normal menu traversal was being performed).

When a function is restricted, the access control function determines if the user has permission to access the function. Normally the icons for the functions the user is not permitted to access are not displayed in the GUI.

The following table summarizes the access controls and configuration parameters used by the TOE to control user access to the SFP functions provided by the TOE. Additional details for each function are provided in subsequent sections.

Table 21: TOE User Function Access Control

Function	Access Control Rules	Configuration Parameter Rules
Print	Network print jobs can always be submitted. The job is held until released by a user who is authorized for the Held Jobs Access function and has the same userid as was specified in the SET USERNAME PJL statement. Network print jobs without a PJL SET USERNAME statement are automatically deleted after the expiry period for held jobs.	Allowed

The following SFRs satisfies Access Control.

FDP_ACC.1 and FDP_ACF.1	Access to user functions is controlled as specified in these SFRs.

6.1.2.1 Printing

Submission of print jobs from users on the network is always permitted. Jobs that do not contain a PJL SET USERNAME statement are discarded after the configured held jobs expiry period. Submitted jobs are always held In the TOE until released or deleted by a user authorized for the appropriate access control and who's userid matches the username specified when the job was submitted. Users are able to display the queue of their pending print jobs. If a held job is not released within the configured expiration time, the job is automatically deleted.

In the evaluated configuration, the setdevparams, setsysparams and setuserparams Postscript operators are made non-operational so that the Postscript DataStream cannot modify configuration settings in the TOE.

6.1.3 Encryption

All configuration data in flash is encrypted using 256-bit AES. Encryption of flash is automatically enabled upon receipt of the printer from the factory. There is no administrator action required to enable printer encryption. All TSF configuration data is automatically encrypted (AES-CBC) as it is written to flash and automatically decrypted when the contents are read.

A common key is used to encrypt flash data. This key is generated using the internal random number generator during initial installation of the HCD firmware. Details of the key chain for the key are provided in the ancillary Key Management Description document. The random number generator function conforms to NIST SP 800-90A Revision 1 using CTR_DRBG(AES) and is seeded with a minimum of 256 bits of entropy by a single hardware source described in the ancillary Entropy document.

The encryption key is specific to the SFP. Section 6.1.9 provides information concerning destruction of keys stored in flash memory.

The following SFRs satisfy Encryption.

FCS_CKM.1/SKG	An AES-256 key is generated for encryption of flash configuration data.
FCS_CKM_EXT.4	The keys are destroyed when an administrator commands the decommission process to be performed.
FCS_CKM.4	Information regarding key destruction is provided in the KMD.
FCS_COP.1/StorageEncryption	Document and configuration data is encrypted using AES-CBC-256.
FCS_COP.1/DataEncryption	TSF configuration data in flash is encrypted using AES-CBC-256.

FCS_KYC_EXT.1	A key chain consisting of a single key is used. Details of the key chain are provided in the ancillary Key Management Description document. The key chain supports DEK outputs of no fewer than 256 bits.
FDP_DSK_EXT.1	All TSF is transparently encrypted in Flash. Flash encryption cannot be disabled. One Flash partition is dedicated to configuration data. The other Flash partitions are not encrypted.
FPT_KYP_EXT.1	Details of the key chain for the key are provided in the ancillary Key Management Description document.

6.1.4 Trusted Communications

During TOE installation, a 3072-bit self-signed certificate for the device is generated in accordance with NIST SP 800-56B Revision 1 ("Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA- based key establishment schemes).

IPSec with ESP operating in transport mode is required for all network datagram exchanges of any type with remote IT systems. This includes the following IT systems:

- Workstations submitting print jobs
- Workstations initiating connections to the web interface
- Remote Syslog server
- KDC
- LDAP server (including Active Directory)
- OCSP server
- NTS

IPSec provides confidentiality, integrity and authentication of the endpoints. Supported encryption options for IKE and ESP is AES-CBC-256. SHA-256 and SHA-384 are supported for HMACs. AES-CBC-256 may only be used if the IKE negotiation also selects AES-CBC-256.

ISAKMP and IKEv1/v2 are used to establish the Security Association (SA) and session keys for the IPSec exchanges. For IKEv1, Main Mode is always used for Phase 1 exchanges (Aggressive Mode is never used). No configuration is necessary. Diffie-Hellman is used for the IKE Key Derivation Function as specified in RFC2409, using Oakley Group 14 or Group 15. SA lifetimes for both IKEv1 and IKEv2 can be limited to separately configurable times for each phase: 1 to 24 hours for Phase 1, and 1 to 8 hours for Phase 2. IKEv1 complies with RFC2409 AND IKEv2 complies with RFC5996.

When the TOE receives an IKE proposal, it selects the first proposed DH group that matches a DH group configured in the TOE (DH Group 14 and Group 15 as specified in RFC 3526 Section 3 is the only supported group) and the negotiation will fail if there is no match. Similarly, when the TOE initiates the IKE protocol, a proposal is sent with all of the DH groups that are configured. The peer will select the first match from the IKE proposal against its configured DH groups; the negotiation fails if no match is found.

Peer authentication is performed using the RSA algorithm and certificates and/or pre-shared keys.

During the ISAKMP exchange, the TOE requires the remote IT system to provide a certificate or text-based Pre-Shared Keys (PSKs) may be configured by administrators and validated between endpoints. PSKs configured in the system may be 1 to 256 characters in length, composed of the characters specified in FIA_PSK_EXT.1.2, and are conditioned using a pseudo-random function (PRF) using HMAC-SHA2-256 or HMAC-SHA2-384 according to RFC 2409 (for IKEv1) or RFC 5996 (for IKEv2). The key size specified in the SA exchange is 256 bits, the encryption algorithm is AES-CBC, and the Hash Authentication Algorithm is SHA-256 or SHA-384.

The secret value x used in the IKE key exchange using a 256-bit value obtained from the DRBG. Nonces used in IKE exchanges are generated using the random bit generator specified in FCS_RBG_EXT.1, with length at least equal to the security strength of the negotiated Diffie-Hellman group (112 bits for DH Group 14 (2048-bit MODP), 128 bits for DH Group 15 (3072-bit MODP)) and at least half the output size of the negotiated PRF hash (256 bits for HMAC-SHA2-256, 384 bits for HMAC-SHA2-384), with a minimum of 128 bits.

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

- The certificate path is validated, supporting a path length of 3.
- The signature in each certificate in the path, using 2048-bit or 3072-bit RSA digital signature algorithm, is verified using the public key of the issuing CA certificate in the device's trust store.
- The path must terminate with a CA certificate that has been configured as a trusted anchor.
- All CA certificates in the path contain the basicConstraints extension with the CA flag set to TRUE.
- Certificate revocation status is checked using OCSP as specified in RFC 6960. If an OCSP Responder can't be contacted, the certificate is accepted.
- Revocation checking is performed for the entire certificate chain for certificates received from IPsec peers and when certificates are imported.

In received certificates, the SAN: IP Address must be present and is used as the presented identifier. The certificate of the OCSP Responder must contain the OCSP Signing purpose. Validation of the Code Signing, Server Authentication and Client Authentication purposes is not performed by the TOE since TLS is not supported and code updates are not validated via certificates.

X.509 Certificate Signing Requests may be generated, containing Common Name, Organization, Organizational Unit, and Country values along with a generated 3072-bit RSA public key. Responses from a Certificate Authority are validated.

If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded. The Security Policy Database is dynamically built with an accept/protect rule for each of the configured pre-shared keys and certificates, permitting packets from the addresses associated with them, and a default "final rule" to discard all other traffic. Incoming packets are validated against the SPD. Essentially incoming IP datagrams from authorized addresses (with PSKs or certificates) are accepted, and all other IP datagrams are discarded per the default final rule.

If external accounts are defined, LDAP+GSSAPI is used for the exchanges with the LDAP server. Kerberos v5 is supported for exchanges with the LDAP server.

All session keys are stored in dynamic RAM. Any copy of an RSA private key or PSK in RAM is destroyed when power is turned off. Section in 6.1.9 provides information concerning destruction of keys stored in flash memory.

The TOE provides keyed-hashing message authentication services using HMAC-SHA-256 and HMAC-SHA-384, which operate on blocks of 512, 1024 bits respectively, use key sizes of 256 and 384 bits respectively, and yield message digest sizes of 256 and 384 bits respectively. The following SFRs satisfy Trusted Communications.

FCS_CKM.1/AKG	A 3072-bit asymmetric key pair is generated in accordance with NIST SP 800-56B during installation.
FCS_CKM.2	DH Group 14 and Group 15 are used in exchanges with peers to establish IPSec connections.
FCS_CKM_EXT.4	Session keys are destroyed when sessions terminate. PSKs are destroyed when the PSKs are deleted from the configuration by an authorized administrator.
FCS_CKM.4	Session keys are destroyed when power is removed.
FCS_COP.1/ DataEncryption	IPsec traffic is encrypted using AES-CBC-256.
FCS_COP.1/KeyedHash	IPsec uses keyed-hash message authentication codes that are authenticated by the TOE.
FCS_COP.1/Hash	IPsec uses keyed-hash message authentication codes that are authenticated by the TOE.
FCS_IPSEC_EXT.1	IPsec is implemented as described in the preceding text.
FIA_X509_EXT.1	X.509 certificates used in IPsec exchanges are validated.
FIA_X509_EXT.2	X.509 certificates may be used in IPsec exchanges for endpoint authentication.
FIA_X509_EXT.3	X.509 Certificate Signing Requests can be generated.
FCS_RBG_EXT.1	An RBG function conforming to NIST SP 800-90A using CTR_DRBG(AES) is used to generate the asymmetric key pair. Entropy is provided by a hardware source that is described in more detail in the ancillary Entropy document.
FIA_PSK_EXT.1	Text-based PSKs are supported and conditioned using a pseudo-random function (PRF) using HMAC-SHA2-256 or HMAC-SHA2-384 according to RFC 2409 (for IKEv1) or RFC 5996 (for IKEv2).

FTP_ITC.1	Trusted channels using IPsec are supported for authentication servers, remote audit servers, and network time servers.
FTP_TRP.1/Admin	Trusted paths using IPsec are supported for administrators using the web interface.
FTP_TRP.1/NonAdmin	Trusted paths using IPsec are supported for users submitting print jobs.

The following table includes the NIST SP 800-56B Rev. 2 *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*, March 2019 Conformance.

Table 22: NIST SP800-56B Conformance

Section #	"should", "should not", or "shall not"	Implemented accordingly?	Rational for deviation
5.6	should	Yes	n/a
5.8	shall not	Yes	n/a
5.9	shall not (first occurrence)	Yes	n/a
5.9	shall not (second occurrence)	Yes	n/a
6.1	should not	Yes	n/a
6.1	should (first occurrence)	Yes	n/a
6.1	should (second occurrence)	Yes	n/a
6.1	should (third occurrence)	Yes	n/a
6.1	should (fourth occurrence)	Yes	n/a
6.1	shall not (first occurrence)	Yes	n/a
6.1	shall not (second occurrence)	Yes	n/a
6.2.3	should	Yes	n/a
6.5.1	should	Yes	n/a
6.5.2	should	Yes	n/a
6.5.2.1	should	Yes	n/a
6.6	shall not	Yes	n/a
7.1.2	should	Yes	n/a
7.2.1.3	should	Yes	n/a
7.2.1.3	should not	Yes	n/a
7.2.2.3	should (first occurrence)	Yes	n/a
7.2.2.3	should (second occurrence)	Yes	n/a
7.2.2.3	should (third occurrence)	Yes	n/a
7.2.2.3	should (fourth occurrence)	Yes	n/a
7.2.2.3	should not	Yes	n/a
7.2.2.3	shall not	Yes	n/a
7.2.3.3	should (first occurrence)	Yes	n/a
7.2.3.3	should (second occurrence)	Yes	n/a
7.2.3.3	should (third occurrence)	Yes	n/a

Section #	"should", "should not", or "shall not"	Implemented accordingly?	Rational for deviation
7.2.3.3	should (fourth occurrence)	Yes	n/a
7.2.3.3	should (fifth occurrence)	Yes	n/a
7.2.3.3	should not	Yes	n/a
8	should	Yes	n/a
8.3.2	should not	Yes	n/a

6.1.5 Administrative Roles

The TOE provides the ability for authorized administrators to manage TSF data from remote IT systems via a browser session or locally via the touch panel. Authorization is granular, enabling different administrators to be granted access to different TSF data.

Authorized administrators (U.ADMIN) have one or more permissions to access management menus and/or functions (as defined in FMT_SMF.1). The following table provides a correlation between functions and the required permission.

Table 23: Function Correspondence to Permissions

Management Function	Required Permission
User management	Security Menus
Role management	Security Menus
Configuring identification and authentication	Security Menus
Configuring authorization and access controls	Security Menus
Configuring communication with External IT Entities	Network/Ports Menu
Configuring network communications	Network/Ports Menu
Configuring the system or network time source	Network/Ports Menu
Configuring data transmission to audit server	Security Menus
Configuring internal audit log storage	Security Menus
Configure applications	Apps Configuration
Perform firmware updates	Firmware Updates
Configure device functions	Function Configuration Menus
Sanitize device	Out of Service Erase

If defined users have no management permissions, they are considered to have the U.NORMAL role and have no access to management functions or data. When new users are defined, by default they have no associated groups, and therefore no access to management functions or job functions (restrictive default attributes).

Neither the web interface nor the touch panel provide the ability to view the values of PSKs, symmetric keys or private keys for any administrator or user.

The following SFRs satisfy Administrative Roles.

FMT_MOF.1	Administrators with the appropriate permissions have the ability to disable, enable and control the behavior of the specified functions.
FMT_MSA.1	Only administrators with the Security Menus permission may query, modify, delete or create user accounts or groups.
FMT_MSA.3	By default, new users have no group memberships and therefore restrictive permissions.
FMT_MTD.1	Administrator operations on specific TSF data is determined by their permissions as described in Table 18.
FMT_SMF.1	Management functionality for the listed functions is provided to administrators as described in section 5.2.5.5.
FMT_SMR.1	Administrators have one or more permission related to management functionality. Users have job function permissions only.
FPT_SKP_EXT.1	PSKs, symmetric keys and private keys are stored in flash. No mechanism is provided to read PSKs, symmetric keys or private keys.

6.1.6 Auditing

The TOE generates audit event records for security-relevant events. The events that cause audit records to be generated are specified in section Table 15. A time stamp is inserted into each record; reliable time is maintained via internal hardware or NTP. When NTP is used, it must be transmitted over IPsec (all communication with the TOE must use IPsec). A severity level is associated with each type of auditable event; only events at or below the severity level configured by an administrator are generated. Per the evaluated configuration, the severity level must be set to 5 (Notice).

Audit records are stored internally as well as being sent to a configured remote syslog server. Communication with the remote syslog server uses the Syslog protocol with IPsec.

Audit records for Successful Login events include the userid of the user as well as a session identifier. Other audit records include the session identifier, enabling the userid associated with other audit records to be determined via the corresponding Successful Login record. The time field in audit records is supplied by the TOE if internal time is configured by an administrator or by an NTP server if external time is configured.

Audit records sent to the remote syslog server follow the syslog format defined in the Berkeley Software Distribution (BSD) Syslog Protocol (RFC 3164). The TOE supplies the PRI, HEADER, MSG/TAG, and

MSG/CONTENT fields for all messages. The CONTENT portion may contain the following fields (in order, separated by commas):

- Event Number
- ISO 8601 time ([YYYY-MM-DD]T[hh:mm:ss])
- Severity
- Process (same as TAG)
- Remote IPv4 address
- Remote IPv6 address
- Remote Hostname
- Remote Port
- Local Port
- Authentication/Authorization method
- Username
- Setting ID
- Setting's old and new values
- Event name
- Event data

Fields in the CONTENT section that are not relevant for specific events are blank. The remote IPv4 address, remote IPv6 address, remote hostname, remote port, and local port fields are always blank for events resulting from actions at the SFP (e.g., usage of the touch panel).

Audit records are stored in the internal log as they are generated. If the internal audit log storage space usage reaches 98% of capacity, the oldest records are purged until used space is lowered to 80%.

Using the web interface, administrator with the Security Menu permission may upload the audit log in syslog or CSV format to their remote system via the browser connection. The audit log is saved as a local file and may be reviewed by the administrator. These administrators may also clear (empty) the audit log. When this action is performed, an Audit Log Cleared record is generated to note this action. Audit records may not be modified.

No users, or administrators without the Security Menu permission, may view, modify or delete audit records.

The following SFRs satisfy Auditing.

FAU_GEN.1	Audit records are generated for the events and with the content specified in Table 15. Audit records are stored in an internal log and transmitted to a remote syslog server. Storage space allocated for internal audit log storage is 1 MB.
FAU_GEN.2	Users can be associated with audit events performed by identified users.

FAU_SAR.1	Administrators with the Security Menu permission may view the internal audit log via the web interface.
FAU_SAR.2	Only Administrators with the Security Menu permission may view the internal audit log.
FAU_STG.1	Only Administrators with the Security Menu permission may clear the internal audit log. No functionality is provided to modify audit records.
FAU_STG.4	When internal audit log space is exhausted, the oldest records in the log are discarded.
FAU_STG_EXT.1	Audit records are transmitted to a remote audit server via the syslog protocol over IPsec.
FPT_STM.1	The TOE maintains a reliable time stamp via internal hardware or NTP.

6.1.7 Trusted Operation

During initial start-up, the TOE performs self-tests on the cryptographic components.

The following tests are performed during start-up:

- Executable code integrity testing – A digital signature (RSA 2048, SHA256) of the executable code is calculated and compared to a saved value in flash.
- Cryptographic algorithm testing – Uses Known Answer Tests (KATs) to verify proper operation of cryptographic functions.

During the boot cycle, the integrity of the executable code is validated. During manufacturing, write-once fuses are programmed with a hash of Xerox's public code signing key. The boot ROM will refuse to load any code that is not signed by the key whose hash does not match that which was programmed at manufacturing.

At power on, the boot ROM looks for an image description table on the designated boot device. The image description table provides the size and location of the next stage boot loader (g2-loader), a signature of that data, and the public key that generated the signature. The boot ROM loads g2-loader into SRAM, verifies the signature, and verifies that the hash of the public key matches the one programmed in fuses. If all those checks pass, then control is passed to g2-loader.

g2-loader initializes DRAM and some other platform-specific pieces before loading the next stage boot loader, u-boot. g2-loader uses the same image description table and key as the boot ROM for validating u-boot. If its signature checks pass, then control is passed to u-boot.

u-boot then looks for a kernel (and optionally initramfs) to load. The entire cramfs partition is loaded into memory. At the end of the partition is a certificate with signature. u-boot verifies the signature of the entire partition, and verifies that the signature was made by the same key that is baked into u-boot (the

public side of the key is hard-coded in u-boot source code). Control is passed on to the kernel in the boot partition.

The boot partition also contains information that is used by the dm-verity subsystem of the Linux kernel. This information is covered by the same signature as the rest of the boot partition. The kernel uses this information to create a dm-verity device, which the kernel then mounts for the root filesystem. Since changing any part of the root filesystem would invalidate the verity hashes, a read-only filesystem is required, for which Xerox uses squashfs.

If code verification fails, all the imaging and mechanism control blocks of the HCD, as well as network and PCIe functionality, is disabled and the system halts. The only way to proceed is to reboot the HCD. The lack of the normal display on the HCD at boot completion indicates that vendor support should be contacted.

Other code partitions may be mounted by Linux at run-time, in which case a dm-verity device is created and mounted to ensure that the code is trusted.

Any writable filesystems are mounted as noexec so as to avoid inadvertently executing code from them, since any code stored there would not be covered by a trusted signature.

Xerox uses full partition images for code update. That is, the code update file contains the entire partition for the new version of code, as opposed to doing per-file updates or delta-images. When a code update file is received by the device, it is saved to a writable filesystem, and then the device is rebooted into recovery mode (i.e., using the recovery boot and recovery root partitions). This avoids the complexity of rewriting a partition while concurrently running from it.

The code update information is validated in the same manner as described above for operational code – the code must be signed with a public key whose hash matches the value burned into fuses during manufacturing.

During operation, a SHA256 hash is maintained for each executable page. Before any page is loaded into memory, the hash is verified to ensure the code has not been modified since boot.

Administrators may use the web interface to query the current firmware version or supply firmware updates. Firmware updates must be digitally signed, and the TOE verifies the signature before applying the update.

The following SFRs satisfy Trusted Operation.

FCS_COP.1/SigGen	Digital signatures of update files are authenticated before being applied.
FCS_COP.1/Hash	Digital signatures verification relies on hash algorithms supplied by the TOE.
FPT_SBT_EXT.1	On each boot, a hardware-based chain of trust is used to validate the integrity of the executable code.

FPT_TST_EXT.1	A set of self-tests are executed at start-up to verify correct operation of the TOE.
FPT_TUD_EXT.1	Administrators may use the web interface to query the current firmware version and supply signed updates.

6.1.8 Data Clearing and Purging

6.1.8.1 Data Overwrite

D.USER.DOC is not stored on a wear-leveled device.

The TOE overwrites RAM with zeroes upon deallocation of any buffer used to hold user data.

The following SFR satisfies Data Overwrite

FDP_UDU_EXT.1	Document data is overwritten when the file or memory containing the data is released.

6.1.8.2 Data Wiping

An administrator may command the TOE to be sanitized (e.g., prepared for decommissioning). For this operation the flash configuration data is overwritten with ones (flash is a wear-leveled device). In addition, the key for flash configuration data is overwritten with zeroes. This wipes D.TSF from flash storage (which contains no D.USER).

The following SFRs satisfy Data Wiping.

FPT_WIPE_EXT.1	When purging is commanded by an administrator flash storage is overwritten with ones.

6.1.9 Common Functionality Regarding Key Destruction in Flash Memory

Multiple types of keys are stored in flash memory: RSA private keys and PSKs. The flash component performs wear leveling/garbage collection; therefore, physical copies of these keys may continue to exist inside the flash component for some period of time after they have been “overwritten” by the software.

The keys stored in flash are the RSA private keys associated with the device certs and the IPSec PSKs. When a single PSK is modified from the configuration by an administrator, the new value of the same size overwrites the old value. When an administrator requests the TOE to be sanitized (e.g., decommissioning), the location in flash holding the PSKs are overwritten once with ones. Therefore, the visible storage locations for these items from the flash component reflect the overwrites.

The flash component supports the TRIM command and implements garbage collection to destroy the persistent copies of the old storage locations when not actively engaged in other tasks. The file system that maps to the flash component, and on which these keys are stored, also supports the TRIM command and the file system is configured to use it.

6.1.10 CAVP Certificates

The following CAVP certificates apply to the Xerox software for this evaluation.

Table 24: CAVP Certificates

Crypto Function	CAVP Certificate #s	Associated SFRs
AES (CBC)	#A3901, #A3900 (88PA6270 (G2)-64bit)	FCS_COP.1/DataEncryption FCS_COP.1/StorageEncryption FCS_IPSEC_EXT.1 FDP_DSK_EXT.1
DRBG (CTR_DRBG(AES))	#A3901 (88PA6270 (G2)-64bit)	FCS_CKM.1/SKG FCS_RBG_EXT.1
HMAC	#A3901, #A3900 (88PA6270 (G2)-64bit)	FCS_COP.1/KeyedHash FCS_IPSEC_EXT.1
RSA	#A3901 (88PA6270 (G2)-64bit)	FCS_CKM.1/AKG FCS_COP.1/SigGen
SHA	#A3901, #A3900 (88PA6270 (G2)-64bit)	FCS_COP.1/Hash FCS_IPSEC_EXT.1
CVL (IKEv1, IKEv2)	#A3901 (88PA6270 (G2)-64bit)	FCS_IPSEC_EXT.1
Finite field-based scheme	#A3901 (88PA6270 (G2)-64bit)	FCS_CKM.2

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

7. Protection Profile Claims

This ST claims exact conformance to the *collaborative Profile for Hardcopy Devices,* Version 1.0e, 4 March 2024 (HCDcPP) along with all applicable errata and interpretations from the certificate issuing scheme.

The Security Problem Definition of the HCDcPP have been included in section 3 of this ST.

The Security Objectives of the HCDcPP have been included in section 4 of this ST.

All claimed SFRs are defined in the HCDcPP. All mandatory SFRs are claimed. The conditional mandatory FCS_KYC_EXT.1, FDP_DSK_EXT.1, FIA_AFL.1, FPT_KYP_EXT.1, and FTP_TRP.1/NonAdmin SFRs are claimed. The Selection-Based FCS_COP.1/KeyedHash, FCS_COP.1/StorageEncryption, FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, and FIA_X509_EXT.3 are claimed and are consistent with the selections made in the mandatory SFRs that prompt their inclusion. The optional FDP_UDU_EXT.1 and FPT_WIPE_EXT.1 SFRs are claimed.

.

8. Rationale

8.1 Conformance Claim Rationale

This Security Target includes the HCDcPP Security Problem Definition, Security Objectives, and Security Assurance Requirements. The Security Target does not add, remove, or modify any of these items. Security Functional Requirements have been reproduced with the Protection Profile operations completed. All selections, assignments, and refinements made on the claimed Security Functional Requirements have been performed in a manner that is consistent with what is permitted by the HCDcPP. The proper set of selection-based requirements have been claimed based on the selections made in the mandatory requirements. Consequently, the claims made by this Security Target are sufficient to address the TOE's security problem.

8.2 TOE Security Objective Rationale

8.2.1 TOE Security Functional Requirements Rationale

The following information is copied from the HCDcPP.

Table 25: TOE Security Functional Requirements Rationale

Objective	Addressed by	Rationale
O.USER_AUTHORIZATION	FDP_ACC.1	This requirement defines an access control policy that governs the authorization required to interact with user data.
	FDP_ACF.1	This requirement defines the rules enforced by the access control policy defined in FDP_ACC.1 to control access to user data.
	FIA_ATD.1	This requirement defines the list of security attributes belonging to individual users that supports user authentication.
	FMT_MSA.1	This requirement enforces restrictions on the subjects that can interact with user data and their security attributes.
	FMT_MSA.3	This requirement defines the default access restrictions that are enforced on user data security attributes if not overridden by specific access control policy rules.

Objective	Addressed by	Rationale
	FMT_SMF.1	This requirement defines the management functions that are provided by the TOE to authorized users.
	FMT_SMR.1	This requirement defines the different security-related roles that the TOE recognizes.
O.USER_I&A	FIA_AFL.1	This requirement defines how many consecutive unsuccessful authentication failures to prove a user's identity trigger actions by the TOE and what those actions will be.
	FIA_PMG_EXT.1	This requirement defines the rules for passwords used by users for purposes of proving their identity to the TOE at the TOE itself.
	FIA_UAU.1	This requirement defines the allowed actions that can be performed on behalf of a user before the user is authenticated and requires users to be authenticated before security functions by the TOE can be performed.
	FIA_UAU.7	This requirement defines what type of feedback to the user is to be provided while authentication is in progress.
	FIA_UID.1	This requirement defines what actions users can perform before being identified by the TOE.
	FIA_USB.1	This requirement defines the rules governing the association of the user's security attributes to a subject acting on the user's behalf.
	FTA_SSL.3	This requirement enforces that the TOE terminates an interactive user session after a defined period of inactivity.
O.ACCESS_CONTROL	FDP_ACC.1	This requirement defines an access control policy that governs the authorization required to interact with user data.
	FDP_ACF.1	This requirement defines the rules enforced by the access control policy

Objective	Addressed by	Rationale
		defined in FDP_ACC.1 to control access to user data.
	FMT_MSA.1	This requirement enforces restrictions on the subjects that can interact with user data and their security attributes.
	FMT_MSA.3	This requirement defines the default access restrictions that are enforced on user data security attributes if not overridden by specific access control policy rules.
	FMT_MTD.1	This requirement defines the roles that can perform specified operations on TSF data.
	FMT_SMF.1	This requirement defines the management functions that are provided by the TOE to authorized users.
	FMT_SMR.1	This requirement defines the different security-related roles that the TOE recognizes.
O.ADMIN_ROLES	FIA_UID.1	This requirement defines what admin actions users can perform before being identified by the TSF.
	FMT_MOF.1	This requirement enforces access control on the admin functions provided by the TOE.
	FMT_SMF.1	This requirement defines the management functions that are provided by the TOE to authorized users.
	FMT_SMR.1	This requirement defines the different security-related roles that the TOE recognizes.
O.UPDATE_VERIFICATION	FCS_COP.1/SigGen	This requirement defines the cryptographic algorithms that must be applied to generate digital signatures that are used verify the integrity of software/firmware upgrade files for the TOE.
	FCS_COP.1/Hash	This requirement defines the cryptographic algorithms that must be

Objective	Addressed by	Rationale
		applied to generate cryptographic hash values that are used to verify the integrity of software/firmware upgrade files for the TOE.
	FPT_TUD_EXT.1	This requirement defines the ability of the admin to initiate and verify firmware/software updates to the TOE.
O.TSF_SELF_TEST	FPT_TST_EXT.1	This requirement enforces the use of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TOE.
O.COMMS_PROTECTION	FCS_CKM.1/SKG	This requirement generates the symmetric keys needed to encrypt data being transmitted to/from the TOE.
	FCS_CKM.2	This requirement provides the methods for performing key establishment between the TOE and IT entity that data is to be transferred either to the TOE or from the TOE.
	FCS_CKM_EXT.4	This requirement enforces that all plaintext secret and private cryptographic keys and cryptographic critical security parameters must be destroyed when no longer needed.
	FCS_CKM.4	This requirement enforces the methods that must be used to destroy all cryptographic keys.
	FCS_COP.1/DataEncryption	This requirement defines the cryptographic algorithms that must be applied to encrypt/decrypt data that is to be transmitted to/from the TOE.
	FCS_COP.1/SigGen	This requirement defines the cryptographic algorithms that must be applied to generate digital signatures that help to verify the integrity of data transmitted to/from the TOE.
	FCS_COP.1/Hash	This requirement ensures the use of strong hash mechanisms.
	FCS_RBG_EXT.1	This requirement defines the random bit generation mechanisms that must

Objective	Addressed by	Rationale
		be applied to generate cryptographic keys and cryptographic critical security parameters.
	FPT_SKP_EXT.1	This requirement enforces the prevention of reading all pre-shared keys, symmetric keys, and private keys.
	FTP_ITC.1	This requirement provides for a trusted communications channel to transmit the user and TSF data between the TOE and a trusted external IT entity.
	FTP_TRP.1/Admin	This requirement provides for a trusted communications path between the TOE and the admin
	FCS_IPSEC_EXT.1	This requirement defines the IPsec protocol for the secure transmission of user and TSF data between the TOE and a trusted external IT entity.
	FCS_COP.1/KeyedHash	This requirement defines the cryptographic algorithms that must be applied to perform keyed-hash message authentication.
	FIA_PSK_EXT.1	This requirement defines the components of pre-shared keys for the IPsec protocol.
	FIA_X509_EXT.1	This requirement defines the rules for the validation of X.509 certificates.
	FIA_X509_EXT.2	This requirement defines the use of X.509 certificates for authentication of the protocols used for secure transmission of user and TSF data between the TOE and a trusted external IT entity.
	FIA_X509_EXT.3	This requirement defines the rules for a certificate request for an X.509 certificate.
	FCS_CKM.1/AKG	This requirement defines the cryptographic algorithms that must be applied to generate asymmetric cryptographic keys.

Objective	Addressed by	Rationale
	FTP_TRP.1/NonAdmin	This requirement provides for a trusted communications path between the TOE and a user who is not an admin.
O.AUDIT	FAU_GEN.1	This requirement defines the minimum required auditable events and the required contents of each audit record.
	FAU_GEN.2	This requirement enforces associating each auditable event with the identity of the user that caused the event
	FAU_SAR.1	This requirement provides for the reading of audit records in an interpretable manner.
	FAU_SAR.2	This requirement enforces only allowing users with explicit read- access to read audit records.
	FAU_STG.1	This requirement enforces protection of stored audit records from unauthorized deletion or modification.
	FAU_STG.4	This requirement defines actions to be taken when the audit log is full.
	FAU_STG_EXT.1	This requirement provides for the transmission of audit log records to a trusted external IT entity over a trusted communications channel.
	FPT_STM.1	This requirement provides reliable system time services that are used to provide time stamps on audit log records.
	FTP_ITC.1	This requirement provides for a trusted communications channel to transmit the audit log records between the TOE and a trusted external IT entity.
O.STORAGE_ENCRYPTION	FCS_CKM.1/SKG	This requirement generates the symmetric keys needed to encrypt data being stored on the TOE.
	FCS_CKM_EXT.4	This requirement enforces that all plaintext secret and private cryptographic keys and cryptographic

Objective	Addressed by	Rationale
		critical security parameters must be destroyed when no longer needed.
	FCS_CKM.4	This requirement enforces the methods that must be used to destroy all cryptographic keys.
	FCS_COP.1/Hash	This requirement defines the cryptographic algorithms that must be applied to generate cryptographic hash values that are used verify the integrity of user and TSF data stored on the TOE.
	FCS_COP.1/DataEncryption	This requirement defines the cryptographic algorithms that must be applied to encrypt/decrypt user and TSF data.
	FCS_RBG_EXT.1	This requirement defines the random bit generation mechanisms that must be applied to generate cryptographic keys and cryptographic critical security parameters used to protect the confidentiality and integrity of user and TSF data stored on the TOE.
	FCS_COP.1/StorageEncryption	This requirement defines the cryptographic algorithms that must be applied to encrypt/decrypt user and TSF data stored on the TOE.
	FCS_RBG_EXT.1	This requirement defines the random bit generation mechanisms that must be applied to generate cryptographic keys and cryptographic critical security parameters used to protect the confidentiality and integrity of user and TSF data stored on the TOE.
	FCS_KYC_EXT.1	This requirement defines the rules for creating a key chain to unlock a self-encrypting drive.
	FDP_DSK_EXT.1	This requirement defines the rules for the protection of user and TSF data stored on the TOE.

Objective	Addressed by	Rationale
O.KEY_MATERIAL	FPT_KYP_EXT.1	This requirement defines the rules for the protection of cryptographic keys and key material.
O.IMAGE_OVERWRITE (optional)	FDP_UDU_EXT.1	This requirement enforces the overwriting of user document data stored on the TOE after each job is processed or cancelled.
O.WIPE_DATA (optional)	FCS_CKM_EXT.4	This requirement enforces that all plaintext secret and private cryptographic keys and cryptographic critical security parameters must be destroyed when no longer needed.
	FCS_CKM.4	This requirement enforces the methods that must be used to destroy all cryptographic keys.
	FPT_WIPE_EXT.1	This requirement enforces that customer-supplied user and TSF data is made unavailable at the request of the admin.
O.AUTH_FAILURES	FIA_AFL.1	This requirement defines how many consecutive unsuccessful authentication failures to prove a user's identity trigger actions by the TOE and what those actions will be.
O.FW_INTEGRITY	FPT_SBT_EXT.1	This requirement defines how the integrity of firmware/software at boot time is to be verified via chains of trust, each one anchored in its own root of trust.
	FCS_COP.1/Hash	This requirement ensures the use of strong hash mechanisms.
O.STRONG_CRYPTO	FCS_CKM.1/SKG	This requirement ensures the generation of strong symmetric keys.
	FCS_CKM.2	This requirement ensures the use of strong key establishment mechanisms.
	FCS_COP.1/DataEncryption	This requirement ensures the use of strong methods to perform data encryption/decryption.

Objective	Addressed by	Rationale
	FCS_COP.1/SigGen	This requirement ensures the use of strong digital signature services.
	FCS_COP.1/Hash	This requirement ensures the use of strong hash mechanisms.
	FCS_RBG_EXT.1	This requirement ensures the use of strong random bit generation mechanisms.
	FPT_STM.1	This requirement provides reliable system time services that may be used as inputs to cryptographic functions.
	FCS_COP.1/StorageEncryption	This requirement ensures the use of strong methods to perform data encryption/decryption.
	FCS_IPSEC_EXT.1	This requirement defines the implementation of IPsec using strong cryptography.
	FCS_COP.1/KeyedHash	This requirement ensures the use of strong methods to perform keyed-hash message authentication.
	FCS_CKM.1/AKG	This requirement ensures the generation of strong asymmetric keys.
	FCS_KYC_EXT.1	This requirement ensures the use of strong methods to perform key chaining.

8.2.2 TOE Security Assurance Requirements Rationale

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