Xerox Multi-Function Device Security Target

Xerox® WorkCentre® 3655/3655i 2016 Xerox® ConnectKey® Technology

Prepared by:

Xerox Corporation
800 Phillips Road
Webster, New York 14580

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076

Document Version 1.2

Document Version: 1.2 (July 2016).

Table of Contents

List of Figures

List of Tables

1. Introduction

This Security Target (ST) specifies the security claims of the Xerox® WorkCentre® 3655/3655i 2016 Xerox® ConnectKey® Technology in accordance with the requirements of the Common Criteria (CC).

1.1. ST and TOE Identification

Table 1 below presents key identification details relevant to the CC evaluation of the Xerox® WorkCentre® 3655/3655i 2016 Xerox® ConnectKey® Technology.

Table 1: ST and TOE identification

ST Title:	Xerox Multi-Function Device Security Target, Xerox® WorkCentre® 3655/3655i 2016 Xerox® ConnectKey® Technology
ST Version:	1.2
Publication Date:	14 July 2016
Authors:	CSC Security Testing/Certification Laboratories, Xerox Corporation
TOE Identification:	Xerox® WorkCentre® 3655/3655i 2016 Xerox® ConnectKey® Technology System Software: 073.060.075.34540 with patch 905956v2.dlm
EAL:	EAL2+ (ALC_FLR.3)
ST Evaluator:	CSC Security Testing/Certification Laboratories
Keywords:	Xerox, Multi-Function Device, Image Overwrite, WorkCentre, Printer, Scanner, Copier, Facsimile, Fax, Document Server, Document Storage and Retrieval, Disk overwrite, All-In-One, MFD, MFP, ISO/IEC 15408, Common Criteria, FIPS, Protection Profile, Security Target

1.2. TOE Overview

1.2.1. Usage and Security Features

The Target of Evaluation (TOE) is the Xerox multi-function device (MFD) Xerox® WorkCentre® 3655/3655i 2016 Xerox® ConnectKey® Technology. The TOE copies and prints with scan and fax capabilities. The Xerox Embedded Fax Accessory provides local analog fax capability over Public Switched Telephone Network (PSTN) connections and also enables LanFax[1].

Xerox's Workflow Scanning Accessory is part of the TOE configuration. This accessory allows documents to be scanned at the device with the resulting image being sent via email, transferred to a remote file repository, kept in a private (scan) mailbox or placed on a personal USB storage device.

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

Figure 1: Xerox® WorkCentre® 3655/3655i 2016 Xerox® ConnectKey® Technology

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

The TOE provides the following security features:

- **Image overwrite and data purge.** The image overwrite feature overwrites temporary image files created during a copy, print, scan or fax job when those files are no longer needed. Overwrite is also invoked at the instruction of a job owner or administrator and at start-up. The purge feature allows an authorized administrator to permanently delete all customer-supplied data on the TOE. This addresses residual data concerns when the TOE is decommissioned from service or redeployed to a different environment.
- **Hard disk encryption.** The TOE stores temporary image data created during a copy, print, scan and fax job on the single shared hard disk drive (HDD). This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the HDD used for spooling temporary files are encrypted. The encryption key is created on each power-up.
- **Audit.** The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to identified users. The audit logs, which are stored locally in a 15000 entry circular log, are available to TOE administrators and can be exported in comma separated format for viewing and analysis.
- **Network filtering.** The TOE allows filtering rules to be specified for IPv4 network connections based on IP address and port number.
- **Secure communication.** The TOE provides support for a number of secure communication protocols:
    - Transport Layer Security (TLS) support is available for protecting communication over the Web User Interface (Web UI) and SMTP email communications.
    - Secure Shell (SSH) File Transfer Protocol (SFTP) and TLS are available for protecting document transfers to a remote file depository.
    - Internet Protocol Security (IPsec) support is available for protecting communication over IPv4 networks.
    - Kerberos and TLS support are available for protecting communication with a remote authentication server.
- **Authentication & access control.** In the evaluated configuration, the TOE requires users and system administrators to authenticate before granting access to user (copy, print, fax etc) or system administration functions via the Web User Interface (Web UI) or the Local User Interface (LUI). The user or system administrator must enter a username and password at either the Web UI or the LUI. The password is obscured as it is being entered. The TOE provides role based access control as configured by the system administrator.
- **Network authentication.** The TOE supports smart card, Kerberos and Lightweight Directory Access Protocol (LDAP) for network authentication.

- **Self test and integrity verification.** The TOE includes a software image verification feature and Embedded Device Security which employs McAfee software to detect and prevent unauthorized execution and modification of TOE software.

1.2.2. TOE Type

The TOE is an MFD that provides copy and print, document scanning and fax services.

1.2.3. Required Non-TOE Hardware, Software and Firmware

The TOE does not require any additional hardware, software or firmware in order to function as a multi-function device. Additional features require non-TOE support as follows:

- Network security and fax flow features are only useful in environments where the TOE is connected to a network or PSTN.
- Network identification is only available when LDAP or Kerberos remote authentication services are present in the environment.
- Smart card authentication requires Federal Information Processing Standard (FIPS) 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smart cards and readers or equivalent. In support of smart card authentication, a Windows Domain Controller must also be present in the environment.
- The TOE may be configured to reference an NTP server for time.

1.3. TOE Description

1.3.1. Physical Scope of the TOE

The TOE is an MFD (Xerox® WorkCentre® 3655/3655i 2016 Xerox® ConnectKey® Technology) that consists of a printer, copier, scanner, fax and associated administrator and user guidance. The TOE comprises all software and firmware within the MFD enclosure.

Users can determine version numbers and whether the Xerox Embedded Fax Accessory, Xerox Workflow Scan Accessory and Image Overwrite Security Package are installed by reviewing the TOE configuration report.

The administrator and user guidance included in the TOE are listed in Table 2.

Table 2: System User and Administrator Guidance

Title	Version	Date
Xerox® WorkCentre® 3655/3655i Multifunction Printer 2016 Xerox® ConnectKey® Technology System Administrator Guide	1.3	February 2016
Xerox® WorkCentre® 3655/3655i Multifunction Printer 2016 Xerox® ConnectKey® Technology User Guide	1.2	February 2016
Secure Installation and Operation of Your WorkCentre™ 3655/3655i, WorkCentre™5845/5855/5865/5865i/5875/5875i/5890/5890i, WorkCentre™ 5945/5945i/5955/5955i, WorkCentre™ 6655/6655i, WorkCentre™ 7220/7220i/7225/7225i, WorkCentre™ 7830/7830i/7835/7835i/7845/7845i/7855/7855i, WorkCentre™ 7970/7970i 2016 Xerox® ConnectKey® Technology	1.2	July 2016

The TOE's physical interfaces include a power port, an ethernet port, USB ports, serial port, fax ports, LUI with keypad, a document scanner, a document feeder and a document output.

1.3.2. Logical Scope of the TOE

The TOE logical boundary is the operating system software that provides the following security functions:

- Image Overwrite & Purge (TSF_IOW_PURGE)
- Authentication (TSF_ AUT)
- Network Identification (TSF_NET_ID)
- Security Audit (TSF_FAU)
- Cryptographic Operations (TSF_FCS)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- Network Security (TSF_NET_SEC)
- Information Flow Security (TSF_ FLOW)
- Security Management (TSF_FMT)
- User Data Protection – Disk Encryption (TSF_FDP_UDE)

1.3.2.1. Image Overwrite (TSF_IOW_PURGE)

The Immediate Image Overwrite (IIO) function overwrites files created during job processing. The IIO function automatically starts for all abnormally terminated copy,

print, scan and fax jobs stored on the HDD prior to coming on-line at reboot or after a power failure/disorderly shutdown.

The On-Demand Image Overwrite (ODIO) function overwrites the hard drive(s) on-demand of the system administrator. The ODIO function operates in two modes: full ODIO and standard ODIO. A standard ODIO overwrites all files written to temporary storage areas of the HDD. A full ODIO overwrites those files as well as the fax mailbox/dial directory and scan-to-mailbox data.

The Data Purge function at the command of the system administrator overwrites all jobs that are actively being processed by the TOE or are being held on the TOE for later processing; overwrites all jobs and log files that are stored on the hard drive(s); overwrites all local authentication data stored on the internal database; overwrites all customer data stored in address books and accounting databases and resets the fax and copy controller Nonvolatile Memory (NVM) on the TOE to their factory default values.

1.3.2.2. Authentication (TSF_AUT)

A user must authenticate by entering a username and password prior to being granted access to the LUI or the Web UI. While the user is typing the password, the TOE obscures each character entered.

Upon successful authentication, users are granted access to functions based on their role. The system administrator defines the privileges associated to each role.

If configured for local authentication the system requires the system administrator to create each user and assign associated credentials. The system will authenticate the user against an internal database. The TOE may alternatively be configured to use an external authentication store as described by section 1.3.2.3.

The TOE enforces administrator defined session timeout periods for the LUI and Web UI.

1.3.2.3. Network Identification (TSF_NET_ID)

As an alternative to local authentication, the TOE may be configured to refer to an external identity server (a trusted remote IT entity). User credentials entered at the LUI or Web UI are authenticated at the server instead of the TOE. The network authentication services supported by the TOE include: smart card authentication, LDAP v4, Kerberos v5 (Solaris) and Kerberos v5 (Windows 2000/2003/2008).

1.3.2.4. Security Audit (TSF_FAU)

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

1.3.2.5. Cryptographic Operations (TSF_FCS)

The TOE utilizes digital signature generation and verification (RSA), data encryption (TDES, AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC, SHA-1) in support of disk encryption, SFTP, TLS, TLS/HTTPS, TLS/SMTP and IPsec. The TOE also provides random number generation in support of cryptographic operations.

1.3.2.6. User Data Protection – Disk Encryption (TSF_FDP_UDE)

The TOE utilizes data encryption (AES) to support encryption and decryption of designated portions of the hard disk where user image data files may be temporarily stored.

1.3.2.7. User Data Protection – IP Filtering (TSF_FDP_FILTER)

The TOE enforces administrator defined IPv4 filtering rules.

1.3.2.8. Network Security (TSF_NET_SEC)

The TOE supports the following secure communication protocols: TLS for Web UI; SFTP and TLS for document transfers to the remote file depository; IPsec for communication over IPv4; SMTP over TLS for email; and Kerberos and LDAP over TLS for remote authentication.

1.3.2.9. Information Flow Security (TSF_FLOW)

The TOE prevents unintentional transmission of data between its interfaces and the network and/or PSTN to which the TOE is connected.

1.3.2.10. Security Management (TSF_FMT)

The security functions of the TOE are managed by the system administrator from the LUI and WebUI client. User and role management is only accessible via the Web UI.

1.4. Evaluated Configuration

To implement the security features identified in section 1.2.1 of this Security Target, the TOE must be configured in accordance with the Secure Installation and Operation guidance document (see

Table 2).

The following components are included in the evaluated configuration:

- Xerox Embedded Fax Accessory
- Smart card authentication

No claims are made regarding security features that are not explicitly identified in this Security Target.

Please see http://www.xerox.com/information-security/product/enus.html for the latest Xerox security information, bulletins and advisory responses.

2. Conformance Claims

2.1. Common Criteria

The ST is based upon the following, referenced hereafter as [CC]:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 4
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 4

This ST claims the following CC conformance:

- Part 2 extended
- Part 3 conformant

2.2. Protection Profile Claims

None.

2.3. Package Claims

EAL2-augmented (ALC_FLR.3).

3. Security Problem Definition

3.1. Definitions

3.1.1. Users

Users are entities that are external to the TOE and which interact with the TOE. There may be two types of Users: Normal and Administrator, as shown in Table 3.

Table 3: Users

Designation		Definition
U.USER		Any authorized User.
	U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE
	U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP. This ST specifies: • U.ADMINISTRATOR (System Administrator) • U.ADMINISTRATOR (Accounting Administrator) If U.ADMINISTRATOR is specified without identifying the above, then it refers to both roles.

3.1.2. Objects (Assets)

Objects are passive entities in the TOE, that contain or receive information, and upon which Subjects perform Operations. In this Security Target, Objects are equivalent to TOE Assets. There are three types of Objects: User Data, TSF Data, and Functions.

3.1.2.1. User Data

User Data are data created by and for Users and do not affect the operation of the TOE Security Functionality (TSF). This type of data is composed of two objects: User Document Data, and User Function Data, as shown in Table 4.

Table 4: User data

Designation	Definition
D.DOC	User Document Data consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually-stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

3.1.2.2. TSF Data

TSF Data is data created by and for the TOE and might affect the operation of the TOE. This type of data is composed of two objects: TSF Protected Data and TSF Confidential Data. The TSF Data assets for this TOE has been categorized according to whether they require protection from unauthorized alteration (TSF Protected Data) or protection from both unauthorized disclosure and unauthorized alteration (TSF Confidential Data). The data assets have been identified and categorized in Table 5 and Table 6 below.

Table 5: TSF data

Designation	Definition
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

Table 6: TSF data categorization

TSF Protected Data	TSF Confidential Data
Configuration data	Audit Log
Device and network status information and configuration settings	Cryptographic keys
Device service and diagnostic data	X.509 Certificate (TLS)
	User IDs and Passwords
	User Access Permissions
	802.1x Credentials and Configuration
	IP filter table (rules)
	Email Addresses for fax forwarding

Note: TSF data is categorized as:

1. **TSF Protected Data.** Data that should be protected, but does not affect the operational security of the TOE if it is disclosed (D.PROT).
2. **TSF Confidential Data.** Data that does affect the operational security of the TOE if it is disclosed (D.CONF).

3.1.2.3. HCD Functions

Functions perform processing, storage, and transmission of data that may be present in Hardcopy Device (HCD) products (HCD is an IEEE term for MFD). The HCD functions relevant to the TOE are defined in Table 7 below.

Table 7: HCD functions

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

3.1.3. Operations

Operations are a specific type of action performed by a Subject on an Object. In this Security Target, five types of operations are considered: those that result in disclosure of information (Read), those that result in alteration of information (Create, Modify, Delete), and those that invoke a function (Execute).

3.1.4. Channels

Channels are the mechanisms through which data can be transferred into and out of the TOE. In this Security Target, four types of Channels are allowed:

1. **Private Medium Interface.** Mechanisms for exchanging information that use (1) wired or wireless electronic methods over a communications medium

which, in conventional practice, is not accessed by multiple simultaneous Users; or, (2) Operator Panel and displays that are part of the TOE. It is an input-output channel.

2. **Shared-medium Interface.** Mechanisms for exchanging information that use wired or wireless network or non-network electronic methods over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple Users. It is an input-output channel.
3. **Original Document Handler.** Mechanisms for transferring User Document Data into the TOE in hardcopy form. It is an input channel.
4. **Hardcopy Output Handler.** Mechanisms for transferring User Document Data out of the TOE in hardcopy form. It is an output channel.

In practice, at least one input channel and one output channel would be present in any HCD configuration, and at least one of those channels would be either an Original Document Handler or a Hardcopy Output Handler.

3.2. Assumptions

The Security Objectives and SFRs defined in subsequent sections of this ST are based on the condition that all of the assumptions described in this section are satisfied.

Table 8: Assumptions for the TOE

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

3.3. Threats

3.3.1. Threats Addressed by the TOE

This security problem definition addresses threats posed by four categories of threat agents:

1. Persons who are not permitted to use the TOE who may attempt to use the TOE
2. Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.
3. Persons who are authorized to use the TOE who may attempt to access data in ways for which they not authorized.
4. Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this ST address the threats posed by these threat agents. This section describes threats to assets described in section 3.1.2.

Table 9: Threats to user data

Threat	Affected Asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons

Table 10: Threats to TSF data

Threat	Affected Asset	Description
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

3.3.2. Threats Addressed by the IT Environment

There are no threats addressed by the IT Environment.

3.4. Organizational Security Policies

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for security objectives that are commonly desired by TOE Owners in this operational environment, but for which it is not practical to universally define the assets being protected or the threats to those assets.

Table 11: Organizational Security Policies

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.PURGE.DATA	To prevent unauthorized disclosure of customer data stored on the TOE during decommissioning, a function will be provided that makes all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices .

4. Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

1. Security objectives for the TOE, and
2. Security objectives for the environment.

4.1. Security Objectives for the TOE

This section describes the security objectives that the TOE shall fulfill.

Table 12: Security objectives for the TOE

Objective	Definition
O.DOC.NO.DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO.ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO.ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO.ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO.DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO.ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration.
O.AUDIT.STORAGE.PROTECTED	The TOE shall ensure that internal audit records are protected from unauthorized access, deletion and modifications.

Objective	Definition
O.PURGE.DATA	The TOE shall provide a function that makes all User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices when invoked by an authorized administrator.

4.2. Security Objectives for the Operational Environment

This section describes the security objectives that must be fulfilled by IT methods in the IT environment of the TOE.

Table 13: Security objectives for the IT environment

Objective	Definition
OE.AUDIT.STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.
OE.AUDIT.ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.
OE.USER.AUTHENTICATED	The IT environment shall provide support for user identification and authentication and protect the user credentials in transit when TOE operates in remote identification and authentication mode.

4.3. Security Objectives for the Non-IT Environment

This section describes the security objectives that must be fulfilled by non-IT methods in the non-IT environment of the TOE.

Table 14: Security objectives for the non-IT environment

Objective	Definition
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization, and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization, have the training, competence, and time to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.4. Rationale for Security Objectives

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those security objectives counter the threats, enforce the policies, and uphold the assumptions.

Table 15: Completeness of security objectives

	T.DOC.DIS	T.DOC.ALT	T.DOC.ALT	T.PROT.ALT	T.CONF.DIS	T.CONF.ALT	P.USER.AUTHORIZATION	P.AUDIT.LOGGING	P.INTERFACE.MANAGEMENT	P.PURGE.DATA	A.ACCESS.MANAGED	A.USER.TRAINING	A.ADMIN.TRAINING	A.ADMIN.TRUST
O.DOC.NO.DIS	X													
O.DOC.NO.ALT		X												
O.FUNC.NO.ALT			X											
O.PROT.NO.ALT				X										
O.CONF.NO.DIS					X									
O.CONF.NO.ALT						X								
O.USER.AUTHORIZED	X	X	X	X	X	X	X							
O.INTERFACE.MANAGED									X					
O.AUDIT.LOGGED								X						
O.AUDIT.STORAGE.PROTECTED								X						
O.PURGE.DATA										X				
OE.AUDIT.STORAGE.PROTECTED								X						
OE.AUDIT.ACCESS.AUTHORIZED								X						
OE.INTERFACE.MANAGED									X					
OE.USER.AUTHENTICATED	X	X	X	X	X	X	X							
OE.PHYSICAL.MANAGED											X			
OE.USER.AUTHORIZED	X	X	X	X	X	X	X							
OE.USER.TRAINED												X		
OE.ADMIN.TRAINED													X	
OE.ADMIN.TRUSTED														X
OE.AUDIT.REVIEWED								X						

Table 16: Sufficiency of security objectives

Threats. Policies, and Assumptions	Summary	Objectives and rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons	O.DOC.NO.DIS protects D.DOC from unauthorized disclosure
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.DOC.ALT	User Document Data may be altered by unauthorized persons	O.DOC.NO.ALT protects D.DOC from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.FUNC.ALT	User Function Data may be altered by unauthorized persons	O.FUNC.NO.ALT protects D.FUNC from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization

Threats. Policies, and Assumptions	Summary	Objectives and rationale
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons	O.PROT.NO.ALT protects D.PROT from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons	O.CONF.NO.DIS protects D.CONF from unauthorized disclosure
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons	O.CONF.NO.ALT protects D.CONF from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization

Threats. Policies, and Assumptions	Summary	Objectives and rationale
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
P.USER.AUTHORIZATION	Users will be authorized to use the TOE	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization to use the TOE
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration
		O.AUDIT.STORAGE.PROTECTED protects internal audit records from unauthorized access, deletion and modifications
		OE.AUDIT.STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion and modifications
		OE.AUDIT.ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies

Threats. Policies, and Assumptions	Summary	Objectives and rationale
		OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces
P.PURGE.DATA	Administrators are able to purge all user supllied information.	O.PURGE.DATA provides purge function to remove all user supplied information.
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE
A.ADMIN.TRAINING	Administrators are aware of and trained to follow security policies and procedures	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUSTED establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	TOE Users are aware of and trained to follow security policies and procedures	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.

5. Extended Components Definition

This Security Target defines components that are extensions to Common Criteria 3.1 Release 4, Part 2.

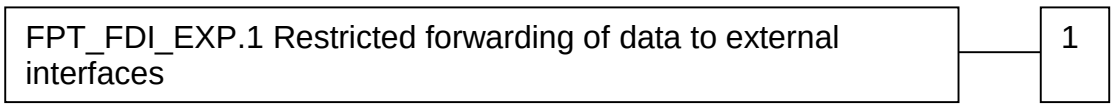
5.1. FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:



FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces, provides for the functionality to require TSF controlled processing of data received over defined external interfaces before this data is sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

The following actions could be considered for the management functions in FMT:

a) definition of the role(s) that are allowed to perform the management activities;

b) management of the conditions under which direct forwarding can be allowed by an administrative role;

c) revocation of such an allowance.

Audit: **FPT_FDI_EXP.1**

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

a) There are no auditable events foreseen.

Rationale:

Quite often a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data is allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e. without processing the data first) between different external interfaces is therefore a function that – if allowed at all – can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Security Target, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and could therefore be placed in either the FDP or FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this lead the authors to define a new family with just one member.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles.

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: list of external interfaces] from being forwarded without further processing by the TSF to [assignment: list of external interfaces].

6. Security Requirements

This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

The CC divides TOE security requirements into two categories:

1. Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
2. Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subsections.

6.1. Conventions

All operations performed on the SFRs or the SARs need to be identified. For this purpose the following conventions shall be used.

- Assignments will be written in [normal text with brackets]
- Selections will be written in *underlined and italic text*.
- Refinements will be written **bold**
- Iterations will be performed on components and functional elements. The component ID defined by the Common Criteria (e.g. FDP_IFC.1) will be extended by an ID for the iteration (e.g. “(FILTER)”). The resulting component ID would be “FDP_IFC.1 (FILTER)”.
- Where an iteration is identified in rationale discussion as “all”, the statement applies to all iterations of the requirement (e.g. “FMT_MTD.1 (all)”)

6.2. TOE Security Policies

This chapter contains the definition of security policies which must be enforced by the TSF.

6.2.1. IP Filter SFP

The security function “User Data Protection – IP Filtering” (TSF_FDP_FILTER) requires that network traffic to and from the TOE will be filtered in accordance with

the rules defined by the system administrator at the Web User Interface configuration editor for IP Filtering. This policy will be enforced on:

- **Subjects.** External entities that send network traffic to the TOE.
- **Information.** All IP-based traffic to and from that destination.

Operations. Pass network traffic.

6.2.2. User Access Control SFP

The Security Function Policy (SFP) described in Table 17 and Table 18 below is referenced by the FDP class SFRs.

Table 17: User Access Control SFP

Object	Attribute	Operation(s)	Subject	Access Control Rule
D.DOC	+PRT	Read	U.NORMAL U.ADMINISTRATOR (Accounting Administrator)	Denied, except for his/her own documents
			U.ADMINISTRATOR (System Administrator)	Allowed, except for documents protected by an optional passcode
		Delete	U.NORMAL, U.ADMINISTRATOR	Denied, except when the associated D.FUNC is deleted.
	+SCN	Read, Delete	U.NORMAL, U.ADMINISTRATOR	Denied, except for his/her own documents
	+CPY	Read, Delete	U.NORMAL, U.ADMINISTRATOR	Denied, except for his/her own documents
	+faxIN	Read, Delete	U.ADMINISTRATOR (System Administrator)	Allowed
		Read, Delete	U.NORMAL U.ADMINISTRATOR (Accounting Administrator)	Denied
	+faxOUT	Read, Delete	U.NORMAL, U.ADMINISTRATOR	Denied, except for his/her own documents
	+DSR and +SCN	Read, Delete	U.NORMAL U.ADMINISTRATOR (Accounting Administrator)	Denied, except for his/her own documents

Object	Attribute	Operation(s)	Subject	Access Control Rule
			U.ADMINISTRATOR (System Administrator)	Allowed
D.FUNC	Any Attribute, except +CPY	Modify	U.NORMAL, U.ADMINISTRATOR	Denied
	+PRT	Delete	U.NORMAL	Denied, except for his/her own documents
			U.ADMINISTRATOR	Allowed
	+SCN	Delete	U.NORMAL, U.ADMINISTRATOR	Denied
	+CPY	Delete, Modify	U.NORMAL, U.ADMINISTRATOR	Denied, except for his/her own documents
	+faxIN	Delete	U.NORMAL, U.ADMINISTRATOR	Denied
	+faxOUT	Delete	U.NORMAL U.ADMINISTRATOR (Accounting Administrator)	Denied
	+faxOUT	Delete	U.ADMINISTRATOR (System Administrator)	Allowed

Table 18: Attributes Definition

Designation	Definition
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+faxIN	Indicates data that are associated with an inbound (received) fax job.
+faxOUT	Indicates data that are associated with an outbound (sent) fax job.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

Application Note: A document (D.DOC) is “owned” by a User (U.User) if that document was created or submitted to the TOE by that User. The only exception are documents received as fax (D.DOC +faxIN), for which the system administrators are considered as the owner.

Application Note: Access control rules for the "Create" Operation are not specified because typically, any authorized U.User can create his/her own documents and cannot create documents that are owned by another User.

6.2.3. TOE Function Access Control SFP

Users (U.NORMAL) require explicit authorization from system administrators (U.ADMINISTRATOR (System Administrator)) for them to be allowed to perform the following TOE Functions via the Web UI or the LUI:

- Print (PRT)
- Scan (SCN)
- Fax (faxIN / faxOUT)
- Copy (CPY)
- Document Storage and Retrieval (DSR)

Any User who is authorized to establish a connection with the TOE through the ethernet port is able to perform the following TOE functions:

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

6.3. Security Functional Requirements

The TOE satisfies the SFRs identified in Table 19. The rest of this section contains a description of each component and any related dependencies.

Table 19: TOE security functional requirements

Functional Component ID	Functional Component Name
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_COP.1	Cryptographic operation
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution

Functional Component ID	Functional Component Name
FCS_CKM.4	Cryptographic key destruction
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles
FPT_FDI_EXP.1	Restricted forwarding of data to external interfaces
FPT_STM.1	Reliable time stamps
FTA_SSL.3	TSF-initiated termination
FTP_ITC.1	Inter-TSF trusted channel

6.3.1. Class FAU: Security audit

6.3.1.1. FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

- Start-up and shutdown of the audit functions;
- All auditable events for the ***not specified*** level of audit; and
- [all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 20].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [for each Relevant SFR listed in Table 20: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required),
- And the following audit attribute:
    - Entry number (an integer value from 1 to the number of entries in the audit log)]

Table 20: Audit data requirements

Auditable Event	Relevant SFR	Audit Level	Additional Information
Job completion	FDP_ACF.1	Not specified	Type of job
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1	Basic	None required
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1	Basic	Attempted user identity, if available
Use of the management functions	FMT_SMF.1	Minimum	None required
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required
Changes to the time	FPT_STM.1	Minimum	None required
Failure of the trusted channel functions	FTP_ITC.1	Minimum	Non required

6.3.1.2. FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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.

6.3.1.3. FAU_STG.1 Protected audit trail storage

Hierarchical to: None.

Dependencies: FAU_GEN.1 Audit data generation

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.

6.3.1.4. FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3.

Dependencies: FAU_STG.1 Protected audit trail storage

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

6.3.2. Class FCO: Communication

There are no Class FCO security functional requirements for this ST.

6.3.3. Class FCS: Cryptographic support

6.3.3.1. FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [the cryptographic operations listed in the Cryptographic Operations column of Table 21] in accordance with a specified cryptographic algorithm [the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 21] and cryptographic key sizes [the cryptographic key sizes listed in the Key Sizes (bits) column of Table 21] that meet the following: [the list of standards in the Standards column of Table 21].

Table 21: Cryptographic operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards & Certs.*
Symmetric encryption and decryption	Triple DES (CBC)	168	SP 800-67 OpenSSL: cert #1223 Mocana: cert #1006
	AES (CBC)	128 256	FIPS 197 OpenSSL: cert #1884 Mocana: cert #1505
Digital signature generation and verification	RSA	2048	FIPS 186-3 OpenSSL: cert #960 Mocana: cert #738
Message digest	SHA-1	N/A	FIPS 180-3 OpenSSL: cert #1655 Mocana: cert #1353
	SHA-256	N/A	FIPS 180-3 OpenSSL: cert #1655 Mocana: cert #1353
Message authentication	HMAC	96 160	FIPS 198 OpenSSL: cert #1126 Mocana: cert #885
Random number generation	DRBG	N/A	SP800-90A OpenSSL: cert #157 Mocana: cert #64

*Cryptographic Algorithm Validation Program (CAVP) certificates

6.3.3.2. FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [the cryptographic algorithms listed in the Cryptographic Algorithm column of

Table 22] and specified cryptographic key sizes [the cryptographic key sizes listed in the Key Sizes (bits) column of

Table 22] that meet the following: [the standards in the Standards column of

Table 22].

Table 22: Cryptographic key generation

Cryptographic Algorithm	Key Sizes (bits)	Standards
Triple DES (OpenSSL)	168	DRBG: SP800-90A
AES (OpenSSL)	128, 256	DRBG: SP800-90A
RSA (OpenSSL)	2048	DRBG: SP800-90A
Triple DES (Mocana)	168	DRBG: SP800-90A
AES (Mocana)	128, 256	DRBG: SP800-90A

6.3.3.3. FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [the method shown for each related protocol in Table 23] that meet the following: [standards shown in Table 23].

Table 23: Cryptographic key distribution

Related Protocol	Key Distribution Method	Standards
TLS (client server authentication)	RSA encrypted exchange of session keys for TLS handshake	RFC 4366
TLS (public keys)	Digital certificates for public keys	RFC 5280 (certificate format)
IPsec	Diffie-Hellman key exchange	RFC 2631
SFTP	Diffie-Hellman key exchange	RFC 2631

6.3.3.4. FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroizationthat meets the following: [FIPS 140-2 zeroization requirements].

6.3.4. Class FDP: User data protection

6.3.4.1. FDP_ACC.1 (USER) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (USER) The TSF shall enforce the [User Access Control SFP in Table 17] on [the list of users as subjects, objects, and operations among subjects and objects covered by the User Access Control SFP in Table 17].

6.3.4.2. FDP_ACC.1 (FUNC) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (FUNC) The TSF shall enforce the [TOE Function Access Control SFP] on [users as subjects, TOE functions as objects, and the right to use the functions as operations].

6.3.4.3. FDP_ACF.1 (USER) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 (USER) The TSF shall enforce the [User Access Control SFP in Table 17] to objects based on the following: [the list of users as subjects and objects controlled under the User Access Control SFP in Table 17, and for each, the indicated security attributes in Table 17].

FDP_ACF.1.2 (USER) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rules specified in the User Access Control SFP in Table 17 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects].

FDP_ACF.1.3 (USER) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (USER) The TSF shall explicitly deny access of subjects to objects based on the [none].

6.3.4.4. FDP_ACF.1 (FUNC) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 (FUNC) The TSF shall enforce the [TOE Function Access Control SFP] to objects based on the following: [Users and their role based permissions to perform any or all of the following functions: print, scan, copy, fax, document storage and retrieval, access to shared-medium interface].

FDP_ACF.1.2 (FUNC) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [users assigned to a role that is explicitly authorized by U.ADMINISTATOR (System Administrator) to use a function is allowed to access the function].

FDP_ACF.1.3 (FUNC) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (FUNC) The TSF shall explicitly deny access of subjects to objects based on the [none].

6.3.4.5. FDP_IFC.1 (FILTER) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (FILTER) The TSF shall enforce the [IPFilter SFP] on [

- Subjects: External entities that send traffic to the TOE;
- Information: All IP-based traffic to/from that source/destination;
- Operations: send or receive network traffic].

6.3.4.6. FDP_IFF.1 (FILTER) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization.

FDP_IFF.1.1 (FILTER) The TSF shall enforce the [IPFilter SFP] based on the following types of subject and information security attributes: [

- Subjects: External entities that send traffic to the TOE
    - IP address,
- Information: IP Packet

- Source IP address, protocol used (TCP or UDP), destination TCP or UDP port].

FDP_IFF.1.2 (FILTER) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- The source IP address matches a rule in the TOE's rule base
- If configured, the destination transport layer port matches a rule in the TOE's rule base.]

FDP_IFF.1.3 (FILTER) The TSF shall enforce the [implicit allow if no rules have been defined].

FDP_IFF.1.4 (FILTER) The TSF shall explicitly authorize an information flow based on the following rules: [if the rule is the default all].

FDP_IFF.1.5 (FILTER) The TSF shall explicitly deny an information flow based on the following rules: [if there are no rules with matching security attributes or if a rule explicitly denies an information flow].

Application Note: When custom rules have not been defined by the system administrator, the default rule (allow all traffic) will apply. Because it is a wildcard rule, all IP addresses, ports and protocols (either TCP or UDP) will be a match for allowed traffic.

6.3.4.7. FDP_RIP.1(IMAGE) Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_RIP.1.1(IMAGE) The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [D.DOC].

6.3.4.8. FDP_RIP.1(PURGE) Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_RIP.1.1(PURGE) The TSF shall ensure that any previous **customer-supplied** information content of a resource is made unavailable upon the **request of an administrator for** the following objects: [all TSF and User data].

6.3.5. Class FIA: Identification and authentication

6.3.5.1. FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [username, password, role].

6.3.5.2. FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [job requests to be received via printing protocols] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.3.5.3. FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of Authentication

FIA_UAU.7.1 The TSF shall provide only [obscured feedback] to the user while the authentication is in progress.

6.3.5.4. FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [job requests to be received via printing protocols] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.3.5.5. FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [username and role].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on behalf of users: [subjects will be assigned the security attributes of the user that they are acting on behalf of].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes with the subjects acting on behalf of users: [security attributes of subjects acting on behalf of a user will not be changed while an action is in progress and cannot be changed by anyone but U.ADMINISTRATOR (System Administrator)].

6.3.6. Class FMT: Security management

6.3.6.1. FMT_MSA.1 (USER) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (USER) The TSF shall enforce the [User Access Control SFP in Table 17] to restrict the ability to *change_default, modify, delete, [read]* the security attributes [all] to [U.ADMINISTRATOR (System Administrator)].

6.3.6.2. FMT_MSA.1 (FUNC) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (FUNC) The TSF shall enforce the [TOE Function Access Control SFP] to restrict the ability to *change_default, modify, delete, [read]* the security attributes [role and associated access permissions] to [U.ADMINISTRATOR (System Administrator)].

6.3.6.3. FMT_MSA.3 (USER) Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 (USER) The TSF shall enforce the [User Access Control SFP in Table 17] to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (USER) The TSF shall allow the [U.ADMINISTRATOR (System Administrator)] to specify alternative initial values to override the default values when an object or information is created.

6.3.6.4. FMT_MSA.3 (FUNC) Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 (FUNC) The TSF shall enforce the [TOE Function Access Control Policy] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (FUNC) The TSF shall allow the [U.ADMINISTRATOR (System Administrator)] to specify alternative initial values to override the default values when an object or information is created.

6.3.6.5. FMT_MTD.1 (MGMT1) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 (MGMT1) The TSF shall restrict the ability to [*download*] the [audit log] to [U.ADMINISTRATOR (System Administrator)].

6.3.6.6. FMT_MTD.1 (MGMT2) Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 (MGMT2) The TSF shall restrict the ability to *change_default, modify, delete, [read]* the [role and associated permissions] to [U.ADMINISTRATOR (System Administrator)].

6.3.6.7. FMT_MTD.1 (KEY) Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

FMT_MTD.1.1 (KEY) The TSF shall restrict the ability to *modify, delete, [create]* the [

- IPsec Secret Key,
- X.509 Server certificate]

to [U.ADMINISTRATOR (System Administrator)].

6.3.6.8. FMT_MTD.1 (FILTER) Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

FMT_MTD.1.1 (FILTER) The TSF shall restrict the ability to *modify, delete, [create, read]* the [

- IP filter rules
- Fax Forwarding Email Addresses]

to [U.ADMINISTRATOR (System Administrator)].

6.3.6.9. FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- Enable/disable Immediate Image Overwrite (IIO);
- Enable/disable and configure smart card use;
- Enable/disable USB ports;
- Invoke ODIO;
- Invoke data purge function;
- Create a recurrence schedule for ODIO;
- Enable/disable audit function;
- Configure SFTP;
- Transfer the audit records (if audit is enabled) to a remote trusted IT product;

- Configure email addresses for audit exhaustion warnings;
- Enable/disable TLS;
- Create/upload/download X.509 certificates;
- Enable/disable and configure 802.1x;
- Enable/disable and configure IPsec;
- Configure (specify the IP address and/or IP address range, port and port range for remote trusted IT products (presumed) allowed to connect to the TOE via the network interface) IP filtering;
- Enable/disable Disk Encryption;
- Configure network authentication;
- Configure users, roles, privileges and passwords;
- Configure WebUI and LUI session timeout;
- Manage receive fax (job) passcodes;
- Configure the Workflow Scanning Repository;
- Enable/disable and configure fax forwarding to email;
- Configure NTP;
- Configure SMTP over TLS; and,
- Enable/disable and configure Enhanced Device Security].

6.3.6.10. FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles [U.ADMINISTRATOR (System Administrator), U.ADMINISTRATOR (Accounting Administrator), U.NORMAL (Authenticated User / system administrator defined roles containing no administrative privileges), *Nobody*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles, **except for the role "Nobody" to which no user shall be associated**.

Application Note: The TOE implements role based access control that allows the system administrator to define custom roles. The system administrator assigns privileges to roles.

Application Note: The role "Nobody" cannot be assigned to any user. It is included in FMT_SMR.1.1 only because it has been used as a role in other SFRs.

6.3.7. Class FPR: Privacy

There are no Class FPR security functional requirements for this Security Target.

6.3.8. Class FPT: Protection of the TSF

6.3.8.1. FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.3.8.2. Class FRU: Resource utilization

There are no Class FRU security functional requirements for this ST.

6.3.9. Class FTA: TOE access

6.3.9.1. FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [U.ADMINISTRATOR (System Administrator) configurable amount of time in the LUI or on the WebUI].

6.3.10. Class FTP: Trusted paths/channels

6.3.10.1. FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF, another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium interface].

6.4. Explicitly Stated Requirements for the TOE

6.4.1. FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [any external Interface] from being forwarded without further processing by the TSF to [any Shared-medium Interface].

6.5. TOE Security Assurance Requirements

Table 24 lists the security assurance requirements for EAL2+ augmented with ALC_FLR.3.

Table 24: EAL2+ (ALC_FLR.3)

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.3 Systematic flaw remediation (augmentation of EAL2)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction

Assurance Class	Assurance Components
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.6. Rationale for Security Functional Requirements

Table 25 and Table 26 below demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 25: Completeness of security functional requirements

	Objectives										
SFRs	O.DOC.NO.DIS	O.DOC.NO.ALT	O.FUNC.NO.ALT	O.PROT.NO.ALT	O.CONF.NO.DIS	O.CONF.NO.ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.AUDIT.LOGGED	O.AUDIT.STORAGE.PROTECTED	O.PURGE.DATA
FAU_GEN.1									**P**	**P**	
FAU_GEN.2									**P**	**P**	
FAU_STG.1										**P**	
FAU_STG.4										**P**	

	Objectives										
SFRs	O.DOC.NO.DIS	O.DOC.NO.ALT	O.FUNC.NO.ALT	O.PROT.NO.ALT	O.CONF.NO.DIS	O.CONF.NO.ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.AUDIT.LOGGED	O.AUDIT.STORAGE.PROTECTED	O.PURGE.DATA
FCS_COP.1	S	S	S	S	S	S					
FCS_CKM.1	S	S	S	S	S	S					
FCS_CKM.2	S	S	S	S	S	S					
FCS_CKM.4	S	S	S	S	S	S					
FDP_ACC.1 (USER)	**P**	**P**	**P**								
FDP_ACC.1 (FUNC)							**P**				
FDP_ACF.1 (USER)	S	S	S								
FDP_ACF.1 (FUNC)							S				
FDP_IFC.1 (FILTER)								**P**			
FDP_IFF.1 (FILTER)								S			
FDP_RIP.1 (IMAGE)	**P**										
FDP_RIP.1 (PURGE)											**P**
FIA_ATD.1							S				
FIA_UAU.1							**P**	**P**			
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**	**P**	S	S	
FIA_USB.1							**P**				
FMT_MSA.1 (USER)	S	S	S								
FMT_MSA.1 (FUNC)							S				
FMT_MSA.3 (USER)	S	S	S								
FMT_MSA.3 (FUNC)							S				
FMT_MTD.1 (MGMT1)				**P**	**P**	**P**					

SFRs	Objectives										
	O.DOC.NO.DIS	O.DOC.NO.ALT	O.FUNC.NO.ALT	O.PROT.NO.ALT	O.CONF.NO.DIS	O.CONF.NO.ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.AUDIT.LOGGED	O.AUDIT.STORAGE.PROTECTED	O.PURGE.DATA
FMT_MTD.1 (MGMT2)				**P**	**P**	**P**					
FMT_MTD.1 (FILTER)				**P**	**P**	**P**					
FMT_MTD.1 (KEY)				**P**	**P**	**P**					
FMT_SMF.1	S	S	S	S	S	S			S		S
FMT_SMR.1	S	S	S	S	S	S	S				
FPT_STM.1									S	S	
FPT_FDI_EXP.1								**P**			
FTA_SSL.3							**P**	**P**			
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					

Table 26: Sufficiency of security functional requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO.DIS, O.DOC.NO.ALT, O.FUNC.NO.ALT	Protection of User Data from unauthorized disclosure or alteration	**FDP_ACC.1(USER)**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1(USER)	Supports access control policy by providing access control function.
		FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MSA.1(USER)	Supports access control function by enforcing control of security attributes.

Objectives	Description	SFRs	Purpose
		FMT_MSA.3(USER)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	**FDP_RIP.1(IMAGE)**	**Enforces protection by making residual data unavailable.**
O.CONF.NO.DIS O.PROT.NO.ALT O.CONF.NO.ALT	Protection of TSF Data from unauthorized disclosure or alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MTD.1(MGMT1) **FMT_MTD.1(MGMT2)** **FMT_MTD.1 (KEY)** **FMT_MTD.1 (FILTER)**	**Enforces protection by restricting access.**
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
O.USER.AUTHORIZED	Authorization of Normal Users and Administrators to use the TOE	**FDP_ACC.1(FUNC)**	**Enforces authorization by establishing an access control policy.**
		FDP_ACF.1(FUNC)	Supports access control policy by providing access control function.
		FIA_ATD.1	Supports authorization by associating security attributes with users.

Objectives	Description	SFRs	Purpose
		FIA_UAU.1	**Enforces authorization by requiring user authentication.**
		FIA_UAU.7	Supports authorization by protecting passwords.
		FIA_UID.1	**Enforces authorization by requiring user identification.**
		FIA_USB.1	**Enforces authorization by distinguishing subject security attributes associated with user roles.**
		FMT_MSA.1(FUNC)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(FUNC)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMR 1	Supports authorization by requiring security roles.
		FTA_SSL.3	**Enforces authorization by terminating inactive sessions.**
O.INTERFACE.MANAGED	Management of external interfaces	**FDP_IFC.1 (FILTER)**	**Enforces management of external interfaces by establishing an information flow policy for the network and fax interfaces**
		FDP_IFF.1 (FILTER)	Supports management of external interfaces by enforcing information flow rules on the network and fax interfaces

Objectives	Description	SFRs	Purpose
		FIA_UAU.1	**Enforces management of external interfaces by requiring user authentication.**
		FIA_UID.1	**Enforces management of external interfaces by requiring user identification.**
		FTA_SSL.3	**Enforces management of external interfaces by terminating inactive sessions.**
		FPT_FDI_EXP.1	**Enforces management of external interfaces by requiring (as needed) administrator control of data transmission from external Interfaces to Shared-medium Interfaces.**
O.AUDIT.LOGGED	Logging and authorized access to audit events	**FAU_GEN.1**	**Enforces audit policies by requiring logging of relevant events.**
		FAU_GEN.2	**Enforces audit policies by requiring logging of information associated with audited events.**
		FIA_UID.1	Supports audit policies by associating user identity with events.
		FMT_SMF.1	Supports audit policies by requiring functions to enable logging of relevant events.
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.

Objectives	Description	SFRs	Purpose
O.AUDIT.STORAGE.PROTECTED	Logging and authorized access to audit events	**FAU_GEN.1**	**Enforces audit policies by requiring logging of relevant events.**
		FAU_GEN.2	**Enforces audit policies by requiring logging of information associated with audited events.**
		FAU_STG.1	**Enforces the audit policies by preventing unauthorized modification or deletion.**
		FAU_STG.4	**Enforces the audit policies by preventing loss of newer audit trail data.**
		FIA_UID.1	Supports audit policies by requiring user identification
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.
O.DOC.NO.DIS O.DOC.NO.ALT O.FUNC.NO.ALT O.PROT.NO.ALT O.CONF.NO.DIS O.CONF.NO.ALT	Protection of User and TSF Data from unauthorized disclosure or alteration	FCS_COP.1 FCS_CKM.1 FCS_CKM.2 FCS_CKM.4	Supports protection by providing cryptographic operations for secure communication and enforces disk encryption.
		FTP_ITC.1	**Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.**
O.PURGE.DATA	Proteciton of residual user supplied information.	**FDP_RIP.1(PURGE)**	**Enforace protection by enabling administrator to purge all user supplied data.**

Objectives	Description	SFRs	Purpose
		FMT_SMF.1	Supports purge function by enabling administrator to invoke purge.

6.7. Rationale for Security Assurance Requirements

The TOE environment will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE. Agents have limited or no means of infiltrating the TOE with code to effect a change and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.

This ST augments EAL2 with ALC_FLR.3, Systematic flaw remediation. ALC_FLR.3 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place and their inclusion is expected by the consumers of this TOE, and that consumers of this TOE are automatically notified of flaws and changes to the TOE.

6.8. Rationale for Dependencies

6.8.1. Security Functional Requirement Dependencies

Table 27: SFR dependencies satisfied is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

Table 27: SFR dependencies satisfied

Functional Component	Dependency (ies)	Satisfied
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1	Yes
	FIA_UID.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes

Functional Component	Dependency (ies)	Satisfied
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
	FCS_CKM.4	Yes
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	Yes
	FCS_CKM.4	Yes
FCS_CKM.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
	FCS_CKM.4	Yes
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2	Yes
	FCS_CKM.1	Yes
FDP_ACC.1(USER)	FDP_ACF.1	Yes, FDP_ACF.1(USER)
FDP_ACC.1(FUNC)	FDP_ACF.1	Yes, FDP_ACF.1(FUNC)
FDP_ACF.1(USER)	FDP_ACC.1	Yes, FDP_ACC.1(USER)
	FMT_MSA.3	Yes, FMT_MSA.3(USER)
FDP_ACF.1(FUNC)	FDP_ACC.1	Yes, FDP_ACC.1(FUNC)
	FMT_MSA.3	Yes, FMT_MSA.3 (FUNC)
FDP_IFC.1 (FILTER)	FDP_IFF.1	Yes, FDP_IFF.1 (FILTER)
FDP_IFF.1 (FILTER)	FDP_IFC.1	Yes, FDP_IFC.1 (FILTER)
	FMT_MSA.3	No[2]
FDP_RIP.1 (IMAGE)	None	
FDP_RIP.1 (PURGE)	None	
FIA_ATD.1	None	
FIA_UAU.1	FIA_UID.1	Yes
FIA_UAU.7	FIA_UAU.1	Yes

[2] The dependency of FDP_IFF.1 (FILTER) on FMT_MSA.3 is not met because none of these functions support “a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.” (CC Part 2). The TOE does not give system administrators the option of specifying default values, permissive or otherwise. In fact, these features are configured and, with the exception of IP Filter rules, cannot be modified by the system administrator other than to enable or disable them. It is for these reasons that the dependency on FMT_MSA.3 is not and cannot be expected to be met.

Functional Component	Dependency (ies)	Satisfied
FIA_UID.1	None	
FIA_USB.1	FIA_ATD.1	Yes
FMT_MSA.1(USER)	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 (USER)
	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.1(FUNC)	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 (FUNC)
	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.3(USER)	FMT_MSA.1	Yes, FMT_MSA.1(USER)
	FMT_SMR.1	Yes
FMT_MSA.3(FUNC)	FMT_MSA.1	Yes, FMT_MSA.1(FUNC)
	FMT_SMR.1	Yes
FMT_MTD.1(MGMT1)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1(MGMT2)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (FILTER)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (KEY)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	Yes
FPT_STM.1	None	
FPT_FDI_EXP.1	FMT_SMF.1	No[3]
	FMT_SMR.1	No[4]
FTA_SSL.3	None	

[3] For this TOE, the restricted forwarding from the external interfaces to the network controller are architectural design features which cannot be configured, hence the dependencies on FMT_SMF.1 is not met.

[4] For this TOE, the restricted forwarding from the external interfaces to the network controller are architectural design features which cannot be configured; hence the dependencies on FMT_SMF.1 and FMT_SMR.1 are not met.

Functional Component	Dependency (ies)	Satisfied
FTP_ITC.1	None	

6.8.2. Security Assurance Requirement Dependencies

SAR dependencies identified in the CC have been met by this ST as shown in Table 28.

Table 28: EAL2 (augmented with ALC_FLR.3) SAR dependencies satisfied

Assurance Component ID	Dependencies	Satisfied
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	Yes, hierarchically Yes
ADV_FSP.2	ADV_TDS.1	Yes
ADV_TDS.1	ADV_FSP.2	Yes
AGD_OPE.1	ADV_FSP.1	Yes, hierarchically
AGD_PRE.1	None	
ALC_CMC.2	ALC_CMS.1	Yes, hierarchically
ALC_CMS.2	None	
ALC_DEL.1	None	
ALC_FLR.3	None	
ASE_CCL.1	ASE_ECD.1 ASE_INT.1 ASE_REQ.1	Yes Yes Yes, hierarchically
ASE_ECD.1	None	
ASE_INT.1	None	
ASE_OBJ.2	ASE_SPD.1	Yes
ASE_REQ.2	ASE_ECD.1 ASE_OBJ.2	Yes Yes
ASE_SPD.1	None	
ASE_TSS.1	ADV_FSP.1 ASE_INT.1 ASE_REQ.1	Yes, hierarchically Yes Yes, hierarchically
ATE_COV.1	ADV_FSP.2 ATE_FUN.1	Yes Yes
ATE_FUN.1	ATE_COV.1	Yes
ATE_IND.2	ADV_FSP.2	Yes

Assurance Component ID	Dependencies	Satisfied
	AGD_OPE.1	Yes
	AGD_PRE.1	Yes
	ATE_COV.1	Yes
	ATE_FUN.1	Yes
AVA_VAN.2	ADV_ARC.1	Yes
	ADV_FSP.2	Yes
	ADV_TDS.1	Yes
	AGD_OPE.1	Yes
	AGD_PRE.1	Yes

7. TOE Summary Specification

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

7.1. TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Sections 6.3 and 6.4.

- Image Overwrite & Purge (TSF_IOW_PURGE)
- Information Flow Security (TSF_FLOW)
- System Authentication (TSF_AUT)
- Network Identification (TSF_NET_ID)
- Security Audit (TSF_FAU)
- Cryptographic Support (TSF_FCS)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- Network Security (TSF_NET_SEC)
- Security Management (TSF_FMT)
- User Data Protection – Disk Encryption (TSF_FDP_UDE)

7.1.1. Image Overwrite & Purge (TSF_IOW_PURGE)

FDP_RIP.1(IMAGE), FDP_RIP.1(PURGE)

The TOE implements an image overwrite security function (using a three pass overwrite procedure consistent with U.S. Deparment of Defense National Industrial Security Program Operating Manual – DoD 5220.22-M – requirements) to overwrite all temporary files created during processing of jobs, files (images) of completed or deleted jobs or any files that are deleted[5].

The TOE spools and processes documents to be printed or scanned. Temporary files are created as a result of this processing on a reserved section of the hard disk drive. The definition of this reserved section is statically stored within the TOE and

[5] Files are stored inside mailboxes. They may be deleted by their owner through individual file deletions or deletion of the mailbox.

cannot be manipulated. Immediately after the job has completed, the files are overwritten, and this is called Immediate Image Overwrite (IIO).

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

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

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

An ODIO cannot be aborted from either the WebUI or LUI.

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

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

7.1.2. Information Flow Security (TSF_FLOW)

FPT_FDI_EXP.1

The only physical shared-medium interface of the TOE is the network interface.

The TOE controls and restricts the data/information flow from the LUI, document scanner and document feeder to the network interface by brokering all data through an intermidary subsystem. A connectivity subsystem further processes the data before sending it to the network interface.

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

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

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

7.1.3. Authentication (TSF_ AUT)

FIA_ATD.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_USB.1, FMT_SMR.1, FTA_SSL.3

The TOE implements a role based access control system. The TOE ships with three pre-configured roles:

- **System Administrator.** Has access to all pathways, services and features including all management functions on the TOE.
- **Logged-in User.** Non-administrative users who have authenticated to the TOE. The System Administrator may create custom roles for Logged-In Users and assign MFD function privileges.
- **Accounting Administrator.** Has access to all device services and pathways except for the tools pathway (which is used for system administrator functions).

The TOE also maintains a fourth category for Non-Logged-In (unauthenticated) users, enabling the system administrator to specify what functions if any are available to unauthenticated users.

A user must authenticate by entering a username and password prior to being granted access to the LUI or the Web UI. While the user is typing the password, the TOE obscures each character entered.

Upon successful authentication, users are granted access based on their role. Only a system administrator is allowed full access to the TOE including all the system administration functions.

If configured for local authentication the system requires the system administrator to enter a username and password for each user. The system will authenticate the user against an internal database.

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

7.1.4. Network Identification (TSF_NET_ID)

FIA_UAU.7, FIA_UID.1, FIA_USB.1, FMT_SMR.1, FTA_SSL.3

As an alternative to local authentication, the TOE may be configured to refer to an external identity server (a trusted remote IT entity). User credentials entered at the LUI or Web UI are authenticated at the server instead of the TOE. The network authentication services supported by the TOE are: smart card authentication, LDAP v4, Kerberos v5 (Solaris) and Kerberos v5 (Windows 2000/2003/2008).

When a user authenticates using the smart card method a PIN number is used instead of a password. The PIN is authenticated by the smart card. If a smart card is used for authentication, by default the LUI will terminate a session that has been inactive for 6 minutes.

The TOE maintains the username from a successful authentication during the context of the job, and this value is entered into the audit log as the username.

Role based access control is implemented as per section 7.1.3 with access policies either stored locally or on an LDAP repository depending on the chosen configuration.

7.1.5. Security Audit (TSF_FAU)

FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.4, FMT_MTD.1 (MGMT1), FPT_STM.1

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to logged-in users, and each log entry contains a timestamp. The audit logs are only available to TOE administrators and can be downloaded via the web interface for viewing and analysis.

The TOE implements an internal time reference with which to timestamp auditable events. The internal time reference is a hardware based (CPU clock). The system administrator may set the time or configure the TOE to reference an NTP server.

The audit log tracks user identification and authentication, system administrator actions, and failure of trusted channels. By adopting a policy of regularly downloading and saving the audit logs, users can satisfy the tracking requirements for transmission of data outside of the local environment, as required by such legislation as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, etc.

The audit log may be downloaded from the Web UI or the LUI. The system administrator must be logged in to download the audit log.

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

Application Note: For print and LanFax jobs not submitted from the Web UI, the network username associated with the logged in user at the client workstation will be recorded in the audit log.

7.1.6. Cryptographic Operations (TSF_FCS)

FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4

The TOE utilizes digital signature generation and verification (RSA), data encryption (TDES, AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC, SHA) in support of disk encryption, SFTP, TLS/HTTPS, TLS/SMTP and IPsec.

The TOE employs two validated cryptographic modules:

- **Mocana v5.4f (CMVP Cert #1614)** provides cryptographic functions for IPSec and AES used in disk encryption. It implements the AES/CTR DRBG from NIST SP800-90A. When cryptographic keys are no longer required, an API call is made to destroy the key via zeroization as described in Table 4 and Section 11 of the Mocana cryptographic module Security Policy (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1614.pdf).
- **OpenSSL v1.0.1p-fips using OpenSSL FIPS Object Module 2.0 (CMVP Cert #1747)** provides all other cryptographic functions. It implements the AES/CTR DRBG from NIST SP800-90A. When cryptographic keys are no longer required, an API call is made to destroy the key via zeroization as described in Section 4.1 of the OpenSSL cryptographic module Secruity Policy (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf).

In addition to explicit key destruction when keys are no longer required, the TOE also ensure that keys are destroyed at power down. Cryptographic keys are stored in volotile memory which requires power to maintain state. When the TOE is shutdown (or power is suddenly interrupted) power is removed from the volatile memory and all data in the memory along with non-persistant cryptographic keys are destroyed.

7.1.7. User Data Protection – Disk Encryption (TSF_FDP_UDE)

FCS_COP.1, FCS_CKM.1, FCS_CKM.4

The TOE utilizes data encryption (AES) to support encryption and decryption of designated portions of the hard disk where user files may be temporarily stored. The algorithm deployed meets the following standard: AES-CBC-256-FIPS-197. Additional detail on cryptographic functions is provided in section 7.1.6.

7.1.8. User Data Protection – IP Filtering (TSF_FDP_FILTER)

FDP_IFC.1 (FILTER), FDP_IFF.1 (FILTER), FMT_MTD.1 (FILTER)

The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy (IPFilter SFP) is defined by the system administrator through specifying a series of rules to “accept,” “deny,” or “drop” packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE. Additionally rules can be generated specifying filtering options based on port number given in the received packet.

7.1.9. Network Security (TSF_NET_SEC)

FTP_ITC.1

The TOE supports the following secure communication protocols: TLS for Web UI; SFTP and TLS for document transfers to the remote file depository; IPsec for communication over IPv4; SMTP over TLS for email; and Kerberos and LDAP over TLS for remote authentication.

7.1.10. Security Management (TSF_FMT)

FDP_ACC.1 (USER), FDP_ACC.1 (FUNC), FDP_ACF.1 (USER), FDP_ACF.1 (FUNC), FIA_ATD.1, FMT_SMF.1, FMT_MSA.1 (USER), FMT_MSA.1 (FUNC), FMT_MSA.3 (USER), FMT_MSA.3 (FUNC), FMT_MTD.1 (MGMT1), FMT_MTD.1 (MGMT2), FMT_MTD.1 (KEY)

7.1.10.1. Management Security Functions

Section 6.3.6.9 of the ST (FMT_SMF.1.1) provides a list of the security management functions provided by the TOE. Management of the security functions and attributes is restricted to system administrators.

7.1.10.2. Controlling Access to MFD Functions

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

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

7.1.10.3. Copy

Copy has to be performed at the local user interface. A user can only read physical copies of the documents (D.DOC +CPY Read). During job setup, a copy job (D.FUNC +CPY Delete, Modify) or image (D.DOC +CPY Read, Delete) can be read, modified or deleted. Once a job is committed, the job (D.FUNC +CPY Delete, Modify) can only be canceled (deleted) during its execution. Once completed, the job is removed.

7.1.10.4. Print

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

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

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

7.1.10.5. Scan

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

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

7.1.10.6. Fax

Faxes can be submitted at the Local User Interface or remotely as LanFax (through the same interfaces as for printing). During job setup, created document images may be read or deleted (D.DOC +faxOUT Read, Delete). Once a job is submitted, only a system administrator can delete the job before it is fully completed, in the case of delayed send for example (D.FUNC +faxOUT Delete).

Access to receive faxes is restricted to the system administrators (D.DOC +faxIN Read, Delete). All received faxes will be stored locally and assigned a system administrator predefined passcode. The system administrator can print or delete

secure received faxes by entering the appropriate passcode. Once printed, the faxes are automatically deleted. Alternatively, the system administrator may also choose to designate email addresses for receiving fax images. Once the fax job is forwarded as an attachment to an email, the job is automatically deleted.

8. Glossary

For the purposes of this document, the following terms and definitions apply. IEEE Std. 100, *The Authoritative Dictionary of IEEE Standards, Seventh Edition,* should be referenced for terms not defined in this annex.

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

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

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

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

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

Authentication: Security measure that verifies a claimed identity.

Authentication data: Information used to verify a claimed identity.

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

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

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

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

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

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

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

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

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

Hardcopy Device (HCD): A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), “all-in-ones”, and other similar products. See also: multifunction device.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SFR package: A named set of security functional requirements.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Acronyms

For the purposes of this document, the following acronyms and definitions apply. IEEE Std. 100, *The Authoritative Dictionary of IEEE Standards, Seventh Edition,* should be referenced for terms not defined in this annex.

Table 29: Acronyms

Acronym	Definition
ALT	Alteration
CAC	Common Access Card
CC	Common Criteria
CPY	Copy
DHCP	Dynamic Host Configuration Protocol
DIS	Disclosure
DSR	Document Storage And Retrieval
EAL	Evaluation Assurance Level
EIP	Extensible Interface Platform
FIPS	Federal Information Processing Standard
HCD	Hardcopy Device
HDD	Hard Disk Drive
IEEE	Institute Of Electrical And Electronics Engineers
IIO	Immediate Image
IOT	Image Output Terminal
IPP	Internet Printing Protocol
IPsec	Internet Protocol Security
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LPR	Line Printer Remote
LUI	Local User Interface
MFD	Multifunctional Device
MFP	Multifunctional Product / Peripheral / Printer
NVM	Nonvolatile Memory
ODIO	On-Demand Image Overwrite

Acronym	Definition
OSP	Organizational Security Policy
PIV	Personal Identity Verification
PPM	Page Per Minute
PP	Protection Profile
PRT	Print
PSTN	Public Switched Telephone Network
SCN	Scan
SFP	Security Function Policy
SFR	Security Functional Requirement
SMI	Shared-Medium Interface
SSH	Secure Shell
ST	Security Target
Std	Standard
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
USB	Universal Serial Bus

10. Bibliography

[B1] Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4 - Part 1: Introduction and General Model

[B2] Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4 - Evaluation Methodology

[B3] IEEE Std. 100, *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition, New York, Institute of Electrical and Electronics Engineers, Inc.[6]

[6] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org)