Lexmark MS610e, MS810e, MS812e, MS911e, M3150, M5155, M5163, M5170, and CS510 Single Function Printers Security Target

Version 1.11

August 29, 2014

Lexmark International, Inc.
740 New Circle Road
Lexington, KY 40550

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Lexmark International, Inc.
740 New Circle Road
Lexington, KY 40550
http://www.lexmark.com

Various text from clauses 5, 7-9, and 12 reprinted with permission from IEEE, 445 Hoes Lane, Piscataway, New Jersey 08855, from IEEE "2600.2™-2009 Standard for a Protection Profile in Operational Environment B", Copyright © 2009 IEEE. All rights reserved.

REVISION HISTORY

Rev	Description
1.0	August 16, 2012, initial release
1.1	August 24, 2012, updated model numbers and added SMI
1.2	August 28, 2012, corrected the table number reference in FAU_GEN.1
1.3	February 13, 2013, updates for FSP consistency
1.4	March 14, 2013, Correction in Table 24
1.5	April 24, 2013, addressed EORs resulting from AGD and ATE
1.6	May 6, 2013, name change for releasing held print jobs
1.7	May 9, 2013, additional CAVP cert and FAC setting change
1.8	May 15, 2013, updated TOE version and application info
1.9	August 6, 2013, updated TOE version
1.10	January 8, 2014, added an explicit statement regarding syslog transmissions
1.11	August 29, 2014, assurance continuity updates including new model

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

AD ....**Active Directory**
AES ....**Advanced Encryption Standard**
AIO ....**All In One**
BSD ....**Berkeley Software Distribution**
CAC .... **Common Access Card**
CAVP ....**Cryptographic Algorithm Validation Program**
CC ....**Common Criteria**
CM ....**Configuration Management**
EAL ....**Evaluation Assurance Level**
ESP ....**Encapsulating Security Payload**
FTP ....**File Transfer Protocol**
GSSAPI ....**Generic Security Services Application Program Interface**
HTTP ....**HyperText Transfer Protocol**
I&A .... **Identification & Authentication**
IPP ....**Internet Printing Protocol**
IPSec ....**Internet Protocol Security**
IPv4 .... **Internet Protocol version 4**
IPv6 .... **Internet Protocol version 6**
ISO ....**International Standards Orgaization**
IT ....**Information Technology**
KDC ....**Key Distribution Center**
KDF ....**Key Derivation Function**
LAN .... **Local Area Network**
LDAP .... **Lightweight Directory Access Protocol**
MB ....**MegaByte**
MFD ....**Multi-Function Device**
NTP ....**Network Time Protocol**
OSP ....**Organizational Security Policy**
PIV .... **Personal Identity Verification**

PJL ....**Printer Job Language**
PP..**Protection Profile**
RFC ....**Request For Comments**
SASL...**Simple Authentication and Security Layer**
SFP ....**Single Function Printer**
SFR ....**Security Functional Requirement**
SNMP ....**Simple Network Management Protocol**
ST..**Security Target**
TFTP ....**Trivial File Transfer Protocol**
TOE ....**Target of Evaluation**
TSF ....**TOE Security Function**
UI ....**User Interface**
URL ....**Uniform Resource Locator**
USB..**Universal Serial Bus**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Lexmark MS610e, MS810e, MS812e, MS911e, M3150, M5155, M5163, M5170, and CS510 Single Function Printers. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1* and all international interpretations through October 10, 2012. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Lexmark MS610e, MS810e, MS812e, MS911e, M3150, M5155, M5163, M5170, and CS510 Single Function Printers Security Target, version 1.11, August 29, 2014.

1.2 TOE Reference

Lexmark MS610e(LW40.PR4.P439), MS810e(LW40.DN4.P439), MS812e(LW40.DN7.P439), MS911e(LF.SA.P054), M3150(LW40.PR4.P439), M5155(LW40.DN4.P439), M5163(LW40.DN4.P439), M5170(LW40.DN7.P439), and CS510(LW40.VY4.P439) Single Function Printers

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented with ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1.

1.4 Keywords

Hardcopy, Paper, Document, Printer, Residual data, Temporary data, Network interface, Single Function Device, SFP

1.5 TOE Overview

1.5.1 Usage and Major Security Features

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

The major security features of the TOE are:

1. All Users are identified and authenticated as well as authorized before being granted permission to perform any restricted TOE functions.

2. Administrators authorize Users to use the functions of the TOE.

3. User Document Data are protected from unauthorized disclosure or alteration.

4. User Function Data are protected from unauthorized alteration.

5. TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.

6. TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.

7. Document processing and security-relevant system events are recorded, and such records are protected from disclosure or alteration by anyone except for authorized personnel.

1.5.2 TOE type

Miscellaneous (Hard Copy Device)

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE is a complete printer, including the firmware and hardware. To be fully operational, any combination of the following items may be connected to the TOE:

1. A LAN for network connectivity. The TOE supports IPv4 and IPv6.

2. IT systems that submit print jobs to the printer via the network using standard print protocols.

3. An IT system acting as the remote syslog recipient of audit event records sent from the TOE.

4. LDAP server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.

5. Card reader and cards to support Smart Card authentication using Common Access Card (CAC) or Personal Identity Verification (PIV) cards. This component is optional depending on the type(s) of I&A mechanisms used. The supported card readers are:

    a. Omnikey 3121 SmartCard Reader,

    b. Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the above readers (example Omnikey 3021),

    c. SCM SCR 331,

    d. SCM SCR 3310v2.

1.6 TOE Description

The TOE provides a printing function, defined as producing a hardcopy document from its electronic form.

All of the TOE models included in the evaluation are complete printers in a single unit.

All of the printers included in this evaluation provide the same security functionality. Their differences are in the speed of printing and support for color operations. The following tables summarize the technical characteristics of the models.

Table 1 - Technical Characteristics of the TOE Models

Model	Processor	Color/Mono	Pages Per Minute
MS610e	ARM v7 800 MHz	Mono	50
MS810e	ARM v7 800 MHz	Mono	55
MS812e	ARM v7 800 MHz	Mono	70
MS911e	ARM v7 800 MHz	Mono	55
M3150	ARM v7 800 MHz	Mono	50
M5155	ARM v7 800 MHz	Mono	55

Model	Processor	Color/Mono	Pages Per Minute
M5163	ARM v7 800 MHz	Mono	63
M5170	ARM v7 800 MHz	Mono	70
CS510	ARM v7 800 MHz	Color	32

The Target of Evaluation (TOE) is described using the standard Common Criteria terminology of Users, Objects, Operations, and Interfaces. Two additional terms are introduced: Channel describes both data interfaces and hardcopy document input/output mechanisms, and TOE Owner is a person or organizational entity responsible for protecting TOE assets and establishing related security policies. In this document, the terms User and Subject are used interchangeably.

Figure 1 - TOE Model
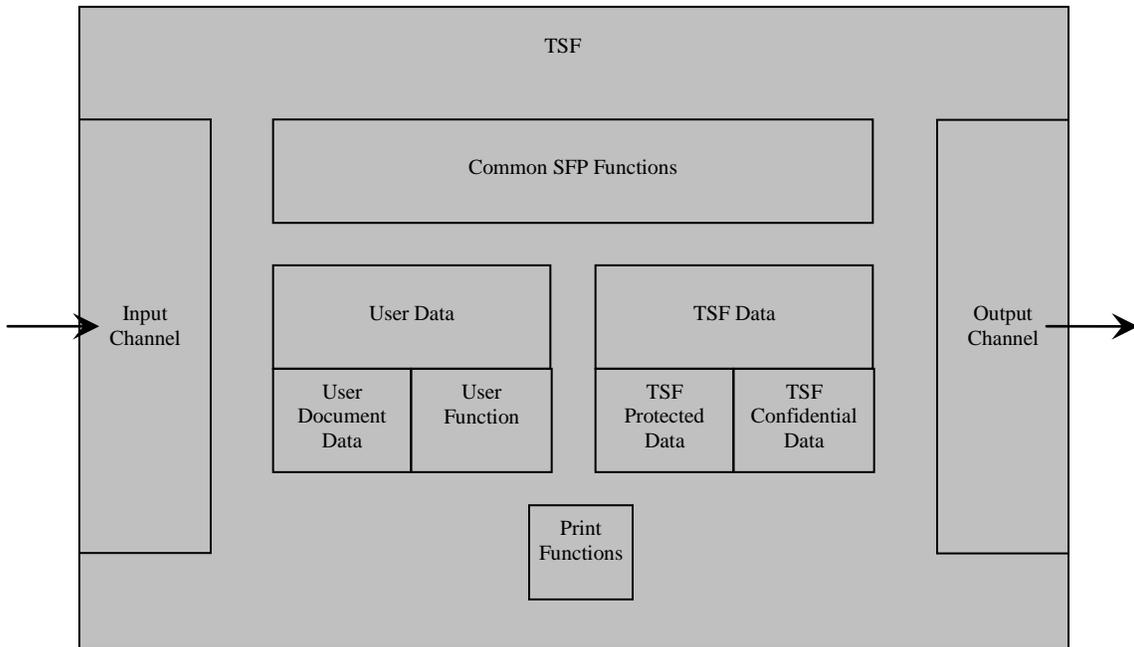
The following prefixes are used to indicate different entity types:

Table 2 -   Notational prefix conventions

Prefix	Type of entity
U.	User
D.	Data
F.	Function
T.	Threat
P.	Policy
A.	Assumption
O.	Objective
OE.	Environmental objective
+	Security Attribute

1.6.1 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.

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. In the remainder of this document, the term "Normal User" is used interchangeably with U.NORMAL. The TOE provides user-level permissions to access specific document processing functions (e.g. print). When it is necessary to distinguish the specific permission, that information is supplied. Otherwise the generic terms identified above are used.
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). In the remainder of this document, the terms "Administrator" and "Authorized Administrator" are used interchangeably with U.ADMINISTRATOR. The TOE provides user-level permissions to access specific management functions. When it is necessary to distinguish the specific permission, that information is supplied. Otherwise the generic terms identified above are used.

1.6.2 Objects (Assets)

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

1.6.2.1 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 types of objects: User Document Data, and User Function Data.

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 in RAM while processing an original document and printed hardcopy output. For this TOE, D.DOC includes: 1. User data contained in jobs submitted from the network for printing
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE. For this TOE, D.FUNC includes: 1. Job information for network print jobs

1.6.2.2 TSF Data

TSF Data are data created by and for the TOE and that might affect the operation of the TOE. This type of data is composed of two types of objects: TSF Protected Data and TSF Confidential Data.

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.

1.6.2.3 Functions

Functions perform processing, storage, and transmission of data that may be present in the TOE. These functions are described in the following table.

Table 6 -   Functions

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output

1.6.3 Operations

Operations are a specific type of action performed by a Subject on an Object. Five types of operations are addressed: 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).

1.6.4 Channels

Channels are the mechanisms through which data can be transferred into and out of the TOE.

Private Medium Interface: mechanism for exchanging information that use (1) wired 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. The touch panel is a private medium interface.

Shared-medium Interface: mechanism for exchanging information that use wired 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. The standard network interface is a shared-medium interface.

Hardcopy Output Handler: mechanism for transferring User Document Data out of the TOE in hardcopy form. It is an output channel. The printer is a hardcopy output handler.

1.7 Physical Boundary

This section provides context for the TOE evaluation by describing the physical boundary of the TOE. The physical boundary of the TOE consists of all of the printer hardware and firmware.

1.8 Logical Boundary

The TOE supports the security functions documented in the following sections.

1.8.1 Audit Generation

The TOE generates audit event records for security-relevant events and transmits them to a remote IT system using the syslog protocol.

1.8.2 Identification and Authentication

The TOE supports I&A with a per-user selection of internal accounts (processed by the TOE) or integration with an external LDAP server (in the operational environment). Smart Card authentication may also be specified for users of the touch panel. A Backup Password mechanism may also be enabled.

1.8.3 Access Control

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

1.8.4 Management

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

1.8.5 D.DOC Wiping

In the evaluated configuration, the TOE automatically overwrites RAM used to store user data as soon as the buffer is released.

1.8.6 Secure Communication

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

1.8.7 Self Test

During initial start-up, the TOE performs self tests on its hardware components and the integrity of the building blocks and security templates.

1.9 TOE Data

1.9.1 TSF Data

Table 7 -   TSF Data

Item	Description	D.CONF	D.PROT
Access Control Authorizations	Access control authorizations specify the restrictions on menus or functions. Items may be configured for no security (accessible to everyone), disabled (not accessible), or restricted by a specified security template.	X	

Item	Description	D.CONF	D.PROT
Account Status	Login status information is associated with all accounts used to authenticate against a building block. For each building block and account, the TOE tracks the number of login failures, time of the earliest login failure, and lock status.	X	
Active Directory Configuration	Configuration information used to join an Active Directory Domain. Once joined, machine credentials are generated and the LDAP+GSSAPI Building Block parameters for communication with the Domain Controller are automatically populated.	X	
Date and Time Parameters	Controls whether the time is tracked internally or from a remote NTP server. If an NTP server is used, it specifies the parameters for communication with the server.		X
Enable Audit	Determines if the device records events in the secure audit log and (if enabled) in the remote syslog.		X
Enable HTTP Server	Enables HTTP(S) server on the TOE.		X
Enable Remote Syslog	Determines if the device transmits logged events to a remote server.		X
Held Print Job Expiration Timer	Specifies the amount of time a received print job is saved for a user to release before it is automatically deleted.		X
Internal Account Building Blocks	The building blocks specify Internal Accounts as the mechanism to be used for I&A or authorizations and specify memberships.	X	
Internal Account Groups	The set of Internal Account Groups may be used to configure group membership for Internal Accounts and authorizations for access controls using Internal Accounts.	X	
IPSec Settings	The configuration parameters for IPSec that require IPSec with ESP for all network communication (IPv4 and/or IPv6) with certificate validation.		X
Internal Accounts Required User Credentials	Specifies whether Internal Accounts use username and password or just username for the I&A process.		X
Job Waiting	Specifies whether a print job may be placed in the Held Jobs queue if the required resources (e.g. paper type) are not currently available, enabling subsequent print jobs to be processed immediately		X
LDAP Certificate Verification	Specifies what verification (if any) should be done on the certificate sent by an LDAP server. Demand specifies that the server certificate is requested; if no certificate is provided or if a bad certificate is provided, the session is terminated immediately. Try indicates the server certificate is requested; if no certificate is provided, the session proceeds normally. If a bad certificate is provided, the session is terminated immediately. Allow indicates the server certificate is requested; if no certificate is provided, the session proceeds normally. If a bad certificate is provided, it will be ignored and the session proceeds normally.		X
LDAP+GSSAPI – Certificate	Specifies whether the default certificate or a specific certificate is required when communicating with an LDAP server.		X
LDAP+GSSAPI – SFP Credentials	Specifies the Username and password to be used when performing LDAP queries.	X	

Item	Description	D.CONF	D.PROT
LDAP+GSSAPI Building Blocks	The building blocks specify LDAP+GSSAPI as the mechanism to be used for I&A or authorizations and specify parameters for retrieving information from an LDAP server (e.g. group names to check, search base, required object names).	X	
LES Applications	Specifies whether enhanced service Java applications may be executed on the TOE. This parameter must be set to "Enable" during installation and is not accessible to administrators during operation.		X
Login Restrictions	Determines how many failed authentications are allowed within the "Failure time frame" value before the offending User Name is prevented from accessing any function protected with the same building block for the duration of the "Lockout time" value. The "Panel Login Timeout" determines how long the operator panel can remain idle on the Home screen before the user is logged off automatically. The "Remote Login Timeout" determines how long web browser sessions can remain idle before the user is logged off automatically.	X	
Network Port	Defines the parameters required for the TOE to communicate via the standard network port		X
Remote Syslog Parameters	Defines the communication to the remote syslog system	X	
Security Reset Jumper	Specifies the behavior of the TOE when a position change of the Security Rest Jumper is detected. No Effect indicates the jumper should be ignored. "No Security" preserves all of the building blocks and templates that a user has defined, but resets each access control to its factory default security level. "Reset to Defaults" deletes all building blocks and templates and resets each access control to its factory default security level.		X
Security Templates	Security Templates are used to configure access controls for restricted functions and menus. Each security template specifies 2 building blocks – one for authentication and one for authorization. The 2 building blocks may be the same. The security template also specifies a set of groups that are authorized to access the associated function or menu.	X	
Simple Kerberos Setup	Defines the KDC Address, KDC Port, and Realm for communication with the KDC. KDC communication is required if the TOE is using the LDAP+GSSAPI mechanism.	X	
Smart Card Authentication Client Building Block	The building block specifies Smart Card Authentication Client as the mechanism to be used for I&A or authorizations and specifies parameters for validating the certificate from the card and retrieving information from Active Directory.	X	
Touch Panel Menu Display - USB Drive	Specifies whether or not the USB Drive icon should be displayed on the touch panel menu.		X
USB Buffer	Disables all activity via the USB device ports.		X
Use Backup Password	Enables access to the Security Menu via the Backup Password	X	

1.9.2 Authentication Data

All the items described in the following table are D.CONF.

Table 8 - Authentication Data

Item	Description
Backup Password	The Backup Password mechanism allows an administrator to access the Security Menu via a web browser session, regardless of the access controls configured for it.
Internal Account Usernames and Passwords	Internal Accounts are used in conjunction with the Internal Account authentication and authorization mechanism. The username and password for each defined account are used with Internal Account authentication.

1.9.3 Security Attributes

All the items described in the following table are D.CONF.

Table 9 - Security Attributes

Item	Description
Group Memberships	The set of group memberships associated with the current session as the result of successful I&A.
Username	The username specified during a successful I&A interaction.

1.9.4 User Data

All the items described in the following table have both a D.DOC and D.FUNC component.

Table 10 - User Data

Item	Description
Held Jobs	Data received via the network interface that is destined for the printer and held until released at the touch panel by the submitter.
Network Print Job	Data received via the network interface and destined for the printer. All network print jobs are held until released.

1.10 Evaluated Configuration

The following configuration options apply to the evaluated configuration of the TOE:

1. The TOE includes the single Ethernet interface that is part of the standard configuration of every printer model. No optional network interfaces are installed.

2. No optional parallel or serial interfaces are installed. These are for legacy connections to specific IT systems only.

3. All USB ports on the printers that perform document processing functions are disabled. In the operational environments in which the Common Criteria evaluated configuration is of interest, the users typically require that all USB ports are disabled. If Smart Card authentication is used, the card reader is physically connected to a specific USB port

during TOE installation; in the evaluated configuration this USB port is limited in functionality to acting as the interface to the card reader. A reader is shipped with the SFP. If Smart card authentication is not used, the card reader may be left unconnected.

4. Operational management functions are performed via browser sessions to the embedded web server or via the management menus available through the touch panel.

5. Access controls are configured for all TSF data so that only authorized administrators are permitted to manage those parameters.

6. All network communication is required to use IPSec with ESP to protect the confidentiality and integrity of the information exchanged, including management sessions that exchange D.CONF and D.PROT. Certificates presented by remote IT systems are validated.

7. Because all network traffic is required to use IPSec with ESP, syslog records sent to a remote IT system also are protected by IPSec with ESP. This is beyond IEEE Std. 2600.2™-2009 requirements for transmission of audit records.

8. Support for AppleTalk is disabled since it does not provide confidentiality and integrity protection.

9. I&A may use Internal Accounts and/or LDAP+GSSAPI on a per-user basis. The Backup Password mechanism may be enabled at the discretion of the administrators. Smart Card authentication may be used for touch panel users. No other I&A mechanisms are included in the evaluation because they provide significantly lower strength than the supported mechanisms.

10. LDAP+GSSAPI and Smart Card authentication require integration with an external LDAP server such as Active Directory. This communication uses default certificates stored in NVRAM; the LDAP server must provide a valid certificate to the TOE. Binds to LDAP servers for LDAP+GSSAPI use device credentials (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific printer. Binds to LDAP servers for Smart Card authentication use user credentials from the card (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific user.

11. Internal Accounts require User ID and password (rather than just User ID).

12. Audit event records are transmitted to a remote IT system as they are generated using the syslog protocol.

13. No Java applications are loaded into the SFP by Administrators. These applications are referred to as eSF applications in end user documentation. The following eSF applications are installed by Lexmark before the TOE is shipped and must be enabled: "eSF Security Manager", "Smart Card Authentication", and "Secure Held Print Jobs".

14. The following eSF applications are installed by Lexmark before the TOE is shipped and must be enabled if smart card authentication is used: "Smart Card Authentication Client", "PIV Smart Card Driver (if PIV cards are used)", "CAC Smart Card Driver (if CAC cards are used)", and "Background and Idle Screen".

15. All other eSF applications installed by Lexmark before the TOE is shipped must be disabled.

16. No option card for downloadable emulators is installed in the TOE.

17. NPAP, PJL and Postscript have the ability to modify system settings. The capabilities specific to modifying system settings via these protocols are disabled.

18. All administrators must be authorized for print functions.

19. All network print jobs are held until released via the touch panel. Every network print job must include a PJL SET USERNAME statement to identify the userid of the owner of the print job. Held print jobs may only be released by an authenticated user with the same userid as specified in the print job.

20. Administrators are directed (through operational guidance) to specify passwords adhering to the following composition rules for Internal Accounts and the Backup Password:

    - A minimum of 8 characters

    - At least one lower case letter, one upper case letter, and one non-alphabetic character

    - No dictionary words or permutations of the user name

21. SNMP support is disabled.

22. Internet Printing Protocol (IPP) support is disabled.

23. All unnecessary network ports are disabled.

The print function may be disabled or restricted, indicating that the functionality is included in the evaluation and may be disabled or restricted to an authorized set of users at the discretion of an administrator

1.11 Rationale for Non-Bypassability and Separation

The TOE is a stand-alone system that includes all hardware and software required for operation. The TOE is not a general-purpose platform; rather it is a specialized platform with strictly controlled functionality made available to the users. By limiting the functionality, the TSF is protected from corruption or compromise. The TOE interfaces are separated into 2 categories – security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user invoked action to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (i.e., they are isolated from the TSF). Multiple simultaneous users are supported, and the TOE enforces separate domains for each process/user to ensure the appropriate attributes and privileges are associated with each process/user.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 4

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Protection Profile Conformance

PP Identification: U.S. Government Protection Profile for Hardcopy Devices (IEEE Std. 2600.2™-2009), dated February 26, 2010, version 1.0, including the augmentations specified by Attachment A of *CCEVS Policy Letter #20* dated 15 November 2010.

PP Conformance: "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B," "2600.2-PRT, SFR Package for Hardcopy Device Print Functions, and "2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B"

This Security Target claims demonstrable conformance to the Security Problem Definition (APE_SPD), Security Objectives (APE_OBJ), Extended Components Definitions (APE_ECD), and the Common Security Functional Requirements (APE_REQ) of the referenced PP.

This TOE performs the F.PRT and F.SMI functions as defined in the referenced PP and claims demonstrable conformance to the SFR packages defined for that function.

Rationale for PP conformance is provided in chapter 8.

2.3 Security Requirement Package Conformance

Security assurance requirement package conformance: EAL2 augmented by ALC_FLR.2

Security functional requirement package conformance: The SFR packages itemized below from the referenced PP.

1. Common Security Functional Requirements
2. 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
3. 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

      A)   assumptions about the environment,

      B)   threats to the assets and

      C)   organisational security policies.

This chapter identifies assumptions as A.*assumption,* threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 11 - Assumptions

A.Type	Description
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.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.
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.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and the Operational Environment.

Table 12 - Threats

T.Type	TOE Threats
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons

3.4 Organisational 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 13 - Organizational Security Policies for the TOE

Name	Definition
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.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 14 - Security Objectives for the TOE

O.Type	Security Objective
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.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.I&A	The TOE shall provide functionality to identify and authenticate users whose accounts are defined internal to the TOE.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.TIME_STAMP	The TOE will provide reliable time stamps for accountability purposes when internal clocks are configured by an administrator.
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.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 15 - Security Objectives of the Operational Environment

OE.Type	Operational Environment Security Objective
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.

OE.Type	Operational Environment Security Objective
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.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.I&A	The operational environment shall provide functionality to identify and authenticate users whose accounts are defined external to the TOE.
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.
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.TIME_STAMP	The Operational Environment will provide reliable time stamps for accountability purposes when NTP is configured by an administrator.
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.

5. Extended Components Definition

5.1 Extended Security Functional Components

5.1.1 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 | 1 |
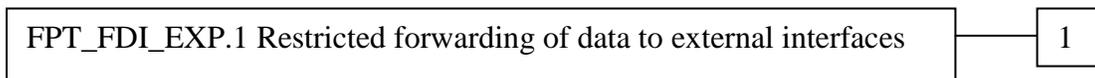
FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface 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:

     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 are 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 Protection Profile, 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 either too implementation-specific for a Protection Profile or 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 it could therefore be placed in either the FDP or the 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 led 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*].

5.2 Extended Security Assurance Components

No extended security assurance requirements are defined.

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

SFR operation completed or partially completed in the PP: Bold

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by letters in parentheses following the component or element (e.g., FAU_ARP.1(A)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

  c) **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 16;** *the additional auditable events specified in Table 16.*

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

  a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

  b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 16: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required;** *the internal event number, ISO 8601 time of the event occurrence, severity, and process.*

Table 16 - Audit data requirements

Auditable event	Relevant SFR	Audit level	Additional Information
SECURE AUDIT TURNED ON/OFF	FAU_GEN.1	n/a	Setting (ON or OFF)

Auditable event	Relevant SFR	Audit level	Additional Information
Job Started (Network print job with PJL SET USERNAME statement)	FDP_ACF.1	Not specified	Userid specified in the PJL SET USERNAME statement, Job identifier
Job Started (Network print job without PJL SET USERNAME statement)	FDP_ACF.1	Not specified	Userid displayed as "Unknown", Job identifier
Job Completed	FDP_ACF.1	Not specified	Job identifier
Job Canceled (By user or via release expiration period)	FDP_ACF.1	Not specified	Job identifier
Expired held job deleted (because it was not released)	FDP_ACF.1	Not specified	
Authorization Failure	FDP_ACF.1	Not specified	Building block type and name
Successful Authorization	FDP_ACF.1	Not specified	Building block type and name
Authentication Failure	FIA_UAU.1, FIA_UID.1	Basic	Building block type and name, attempted user identity
Successful Authentication	FIA_UAU.1, FIA_UID.1	Basic	Building block type and name
Authorization Failure	FMT_MTD.1	Not specified	Building block type and name
Successful Authorization	FMT_MTD.1	Not specified	Building block type and name
Setting change	FMT_MTD.1	Basic	Parameter identifier and new value
Authentication/Authorization Setting CREATION (FAILURE!)	FMT_MTD.1	Basic	Building block type and name
Authentication/Authorization Setting CREATION (Success)	FMT_MTD.1	Basic	Building block type and name
Authentication/Authorization Setting DELETION (FAILURE!)	FMT_MTD.1	Basic	Building block type and name
Authentication/Authorization Setting DELETION (Success)	FMT_MTD.1	Basic	Building block type and name
Authentication/Authorization Setting MODIFICATION (FAILURE!)	FMT_MTD.1	Basic	Building block type and name
Authorization Setting MODIFICATION (Success)	FMT_MTD.1	Basic	Building block type and name
Use of the management functions	FMT_SMF.1	Minimum	None
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None
Time changed	FPT_STM.1	Minimum	None
Time change greater than maximum tolerance	FPT_STM.1	Minimum	None
Time changed due to time source change	FPT_STM.1	Minimum	None
Time changed due to Battery Failure	FPT_STM.1	Minimum	None
User logged out due to timeout	FTA_SSL.3	Minimum	None
Failure of the trusted channel	FTP_ITC.1	Minimum	None

Application Note: The audit for "Use of the management functions" is addressed by the "Setting change" and "Authentication/Authorization Setting" audits. It is included in the audit table above for conformance with the P2600 PP.

Application Note: The audit for "Modifications to the group of users that are part of a role" is addressed by the "Authentication/Authorization Setting" audits. It is included in the audit table above for conformance with the P2600 PP.

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes *2048 bits* that meet the following: *PKCS #1 (CAVP cert. #1233)*.

Application Note: This SFR applies to the RSA public-private key pair generated for the default certificate.

6.1.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *FIPS 140-2 (Vendor Affirmed)*.

6.1.2.3 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform *the operations listed in the table below* in accordance with a specified cryptographic algorithm *multiple algorithms described below* and cryptographic key sizes *as described below* that meet the following: *multiple standards as described below*.

Table 17 - Cryptographic Operations

Algorithm	Operations	Key Size in Bits	Standards
Triple-DES (EDE in CBC mode) (CAVP cert. #1488 & 1489)	Encryption, decryption	168	FIPS 46-3
AES (CBC mode) (CAVP cert. #2379 & 2380)		128, 192, 256	FIPS 197
SHA (CAVP cert. #2049 & 2050)	Hashing	160, 224, 256, 384, 512	FIPS 180-2
HMAC (CAVP cert. #1479 & 1480)	Message authentication coding	128, 160	FIPS 198
RSA (CAVP cert. #1233)	Digital signatures	1024, 2048	PKCS#1
Diffie-Hellman (CAVP cert. #70)	IKEv1 KDF	Group 2 (1024), Group 14 (2048), Group 15 (4096), Group 17 (6144), Group 18 (8192)	SP800-135
DRBG (CAVP cert. #312)	Random number generation	n/a	SP 800-90A

6.1.3 User Data Protection (FDP)

6.1.3.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1(A) The TSF shall enforce the *Common Access Control SFP* on

1. *Subjects: Users (U.USER)*

2. *Objects: Network Print Job*

3. *Operations: Create, View, Modify, Release, Delete*

Application Note: *"Release" refers to releasing held jobs to be printed (at which time they can be read). "View" refers to the ability to see that the job exists (D.FUNC), not to view the user data inside the job. No functionality exists to view the user data inside a job other than printing the document. "Modify" refers to the ability to change job parameters (e.g. number of copies).*

FDP_ACC.1.1(B) The TSF shall enforce the *TOE Function Access Control SFP* on

1. *Subjects: Users (U.USER)*

2. *Objects: TOE Functions - F.PRT, F.SMI*

3. *Operations: Invoke*

6.1.3.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1(A) The TSF shall enforce the *Common Access Control SFP* to objects based on the following:

1. *Subjects: Users (U.USER) – Username, Group memberships*

2. *Objects: Network Print Job*

FDP_ACF.1.2(A) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *the rules specified in the following table*.

Table 18 - Common Access Control SFP Rules

Operation Object	Create	View	Modify	Release	Delete
Network Print Job	Allowed if the submitted job includes a userid in a SET USERNAME PJL statement and the user is a member of an authorized group for the Secure Held Print Jobs access control. Note that all incoming network print jobs are held in the evaluated configuration. The job owner is the userid	Allowed for jobs owned by the user if the user is a member of an authorized group of the security template configured for the Secure Held Print	Allowed for jobs owned by the user if the user is a member of an authorized group of the security template configured for the Secure Held Print	Allowed for jobs owned by the user if the user is a member of an authorized group of the security template configured for the Secure Held Print Jobs access control	Allowed for jobs owned by the user if the user is a member of an authorized group of the security template configured for the Secure Held Print

Operation Object	Create	View	Modify	Release	Delete
	specified in the PJL SET USERNAME statement.	Jobs access control	Jobs access control		Jobs access control

FDP_ACF.1.3(A) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no rules that explicitly authorise access*.

FDP_ACF.1.4(A) The TSF shall explicitly deny access of subjects to objects based on the following rules: *if a listed access control is "Disabled" access is denied.*

FDP_ACF.1.1(B) The TSF shall enforce the *TOE Function Access Control SFP* to objects based on the following:

1. *Subjects: Users (U.USER) – Group memberships*

2. *Objects: TOE Functions (F.PRT, F.SMI) - None*

FDP_ACF.1.2(B) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **the user is explicitly authorized by U.ADMINISTRATOR to use a function**.

FDP_ACF.1.3(B) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no rules that explicitly authorise access*.

FDP_ACF.1.4(B) The TSF shall explicitly deny access of subjects to objects based on the following rules: *if a listed access control is "Disabled" access is denied.*

6.1.3.3 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 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**.

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within the range of 1 to 10 unsuccessful authentication attempts occur related to *accounts within the administratively configured failure time frame.*

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *disable the account for the administratively configured lockout time*.

6.1.4.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1. *Username*

2. *Password*

3. *Associated groups*

4. *User permissions, as specified by associated groups and security template configurations*

5. *Number of consecutive authentication failures*

6. *Time of the earliest authentication failure (since the last successful login if any have occurred)*

7. *Account lock status*

6.1.4.3 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow *submission of network print jobs, and usage of the touch panel and browser sessions with the Embedded Web Server to access menus that have been configured for "no security"* 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.

Application Note: The TOE only performs the authentication for users using Internal Accounts or the Backup Password. When I&A uses LDAP+GSSAPI or Smart Card, authentication is under the control of the LDAP server (and the Smart Card) in the operational environment. For all mechanisms, the TOE restricts access to other functionality until authentication is successful.

6.1.4.4 FIA_UAU.7 Protected Authentication Feedback

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

6.1.4.5 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *usage of the touch panel and browser sessions with the Embedded Web Server to access menus that have been configured for "no security"* 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.

Application Note: The TOE only performs the identification for users using Internal Accounts or the Backup Password. When I&A uses LDAP+GSSAPI or Smart Card, identification is under the control of the LDAP server (and the Smart Card) in the operational environment. For all mechanisms, the TOE restricts access to other functionality until identification is successful.

6.1.4.6 FIA_USB.1 User-Subject Binding

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

1. *Username*

2. *Password*

3. *Associated groups (for Internal Accounts only)*

4. *User permissions*

5. *Building block name used during authentication*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

1. *The username and password are the values supplied by the user.*

2. *The associated groups are the values configured for the user account.*

3. *User permissions are determined by the security templates that include groups in the authorization building blocks that are associated groups of the user.*

4. *The building block name is specified in the security template of the item with access control restrictions that required I&A.*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *the security attributes do not change during a session.*

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to <u>determine the behaviour of, disable, enable, modify the behaviour of</u> the functions *listed in the following table* to *administrators that pass the access control check for the authorization item specified for the listed functions*.

Table 19 - Management of Security Functions Behaviour

Function	Authorization Item	Operations
Audit Generation	Security Menu at the Device, Security Menu Remotely	Disable, enable
Identification & Authentication	Security Menu at the Device, Security Menu Remotely	Determine the behaviour of, disable, enable, modify the behaviour of
Access Control	Security Menu at the Device, Security Menu Remotely	Determine the behaviour of, disable, enable, modify the behaviour of
Management	Security Menu at the Device, Security Menu Remotely	Disable, enable
Secure Communication	Settings Menu at the Device, Settings Menu Remotely	Determine the behaviour of, disable, enable, modify the behaviour of

6.1.5.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the *Common Access Control SFP and TOE Function Access Control SFP* to restrict the ability to <u>query, modify, delete, *create*</u> the security attributes *Username, associated groups and user permissions* to *administrators authorized for access to the Security Menu*.

6.1.5.3 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the *Common Access Control SFP and TOE Function Access Control SFP* to provide <u>restrictive</u> default values for security attributes that are used to enforce the SFP.

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

6.1.5.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *create* the *data identified in the following table* to **the authorized identified roles except U.NORMAL**.

Application Note: The user permission for each TSF data item to determine "authorized identified roles" is identified in the following table.

Table 20 - TSF Data

Item	Authorization Menu Item	Operations
Access Control Authorizations	Security Menu at the Device, Security Menu Remotely	Query, Modify
Active Directory Configuration	Security Menu at the Device, Security Menu Remotely	Create
Backup Password	Security Menu at the Device, Security Menu Remotely	Modify, Delete, Create
Date and Time Parameters	Security Menu at the Device, Security Menu Remotely	Query, Modify
Enable Audit	Security Menu at the Device, Security Menu Remotely	Query, Modify
Enable HTTP Server	Network/Ports Menu at the Device, Network/Ports Menu Remotely	Query, Modify
Enable Remote Syslog	Security Menu at the Device, Security Menu Remotely	Query, Modify
Held Print Job Expiration Timer	Security Menu at the Device, Security Menu Remotely	Query, Modify
Internal Account Building Blocks	Security Menu at the Device, Security Menu Remotely	Query, Modify, Delete, Create
Internal Account Groups	Security Menu at the Device, Security Menu Remotely	Query, Modify, Delete, Create
Internal Account Usernames and Passwords	Security Menu at the Device, Security Menu Remotely	Query, Modify, Delete, Create
Internal Accounts Required User Credentials	Security Menu at the Device, Security Menu Remotely	Query, Modify
Job Waiting	Settings Menu at the Device, Settings Menu Remotely	Query, Modify
LDAP Certificate Verification	Security Menu at the Device, Security Menu Remotely	Query, Modify
LDAP+GSSAPI – Certificate	Security Menu at the Device, Security Menu Remotely	Query, Modify
LDAP+GSSAPI – SFP Credentials	Security Menu at the Device, Security Menu Remotely	Query, Modify
LDAP+GSSAPI Building Blocks	Security Menu at the Device, Security Menu Remotely	Query, Modify, Delete, Create
Login Restrictions	Security Menu at the Device, Security Menu Remotely	Query, Modify
Network Port	Network/Ports Menu at the Device, Network/Ports Menu Remotely	Query, Modify
Remote Syslog Parameters	Security Menu at the Device, Security Menu Remotely	Query, Modify

Item	Authorization Menu Item	Operations
Security Reset Jumper	Security Menu at the Device, Security Menu Remotely	Query, Modify
Security Templates	Security Menu at the Device, Security Menu Remotely	Query, Modify, Delete, Create
Simple Kerberos Setup	Settings Menu at the Device, Settings Menu Remotely	Query, Modify
Smart Card Authentication Client Building Block	Security Menu at the Device, Security Menu Remotely	Query, Modify
Touch Panel Menu Display - USB Drive	Settings Menu at the Device, Settings Menu Remotely	Query, Modify
USB Buffer	Network/Ports Menu Remotely	Query, Modify
Use Backup Password	Security Menu at the Device, Security Menu Remotely	Query, Modify

6.1.5.5 FMT_SMF.1 Specification of Management Functions

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

1. *User management*

2. *Access control management*

3. *Time management*

6.1.5.6 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *defined by the security-relevant permissions in the following table that can be configured in an operational TOE for users via building blocks in security templates for the specific permissions.*

Table 21 - FMT_SMR.1 Detail

Item	Description	Administrators Only?
Network/Ports Menu (and submenus)	Controls access to the Network/ Ports Menu via the Administration Menus	Yes
Reports Menu (and submenus)	Controls access to the Reports Menu via the Administration Menus. This includes information about user jobs, which can't be disclosed to non-administrators.	Yes
Secure Held Print Jobs	In the evaluated configuration, controls which users are permitted to access the Held Jobs menu.	No
Security Menu (and submenus)	Controls access to the Security Menu via the Administration Menus	Yes
Service Engineer Menu (and submenus)	Controls access to any SE menu accessible from the panel, including the Network SE menu	Yes
Settings Menu (and submenus)	Controls access to the Settings Menu via the Administration Menus	Yes

Application Note: *If any permission identified as "Administrators Only" in the table above is associated with a user account, then that user account is implicitly an Administrator (U.ADMINISTRATOR). If no permission identified as "Administrators Only" in the table above is associated with a user account but any permission not identified*

as "Administrator Only" is, then that user account is implicitly a Normal User (U.NORMAL). The role "Nobody" applies to a defined user that has no permissions identified in the table above.

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**.

Refinement Rationale: The SFR is reproduced with the refinement included in the P2600.2 Protection profile..

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

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**.

Application Note: For this TOE, the network interface is the only shared-medium interface.

6.1.6.2 FPT_STM.1 Reliable Time Stamps

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

Application Note: This SFR only applies when the TOE is configured to use internal timestamps. If the TOE is configured to obtain timestamps from an external NTP server, this functionality is provided by that external NTP server in the operational environment.

6.1.6.3 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self tests <u>during initial start-up</u> to demonstrate the correct operation of *<u>the hardware components of the TSF</u>*.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *<u>the security templates and building blocks</u>*.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.7 TOE Access (FTA)

6.1.7.1 FTA_SSL.3 TSF-Initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a *period of time configured by an authorized administrator for touch panel and web browser sessions*.

6.1.8 Trusted Path/Channels (FTP)

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

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 channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit <u>the TSF, another trusted IT product</u> 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**.

Application Note: For this TOE, the network interface is the only shared-medium interface. The TSF requires all IP datagrams entering or leaving the box to use IPSec with ESP (other than the ISAKMP/IKE datagrams used to set up the

security associations). If an incoming IP datagram does not satisfy this rule, the TSF attempts to establish a security association with the remote IT system that originated the datagram.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarized in the following table.

Table 22 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
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.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 23 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_GEN.2	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FCS_CKM.1	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	Satisfied Satisfied
FCS_CKM.4	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1]	Satisfied
FCS_COP.1	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	Satisfied Satisfied
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components.	FDP_ACC.1, FMT_MSA.3	Satisfied Satisfied
FDP_RIP.1	No other components.	None	n/a

SFR	Hierarchical To	Dependency	Rationale
FIA_AFL.1	No other components.	FIA_UAU.1	Satisfied
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.1	No other components.	FIA_UID.1	Satisfied
FIA_UAU.7	No other components.	FIA_UAU.1	Satisfied
FIA_UID.1	No other components.	None	n/a
FIA_USB.1	No other components.	FIA_ATD.1	Satisfied
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied
FPT_FDI_EXP.1	No other components.	FMT_SMR.1	Satisfied
FPT_STM.1	No other components.	None	n/a
FPT_TST.1	No other components.	None	n/a
FTA_SSL.3	No other components.	None	n/a
FTP_ITC.1	No other components.	None	n/a

7. TOE Summary Specification

7.1 Security Functions

7.1.1 Audit Generation

The TOE generates audit event records for security-relevant events. A severity level is associated with each type of auditable event; only events at or below the severity level configured by an administrator are generated.

Each record format follows the syslog format defined in the Berkeley Software Distribution (BSD) Syslog Protocol (RFC 3164). The TOE supplies the PRI, HEADER, MSG/TAG, and MSG/CONTENT fields for all messages. The CONTENT portion may contain the following fields (in order, separated by commas):

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

The time field is supplied by the TOE if internal time is configured by an administrator or by an NTP server if external time is configured.

Fields in the CONTENT section that are not relevant for specific events are blank. The remote IPv4 address, remote IPv6 address, remote hostname, remote port, and local port fields are always blank for events resulting from actions at the SFP (e.g. usage of the touch panel). The events that cause audit records to be generated are specified in section 6.1.1.1 .

As audit event records are generated, they are forwarded to the remote syslog IT system configured by an administrator.

7.1.2 Identification and Authentication

Users are required to successfully complete the I&A process before they are permitted to access any restricted functionality. The set of restricted user functionality is under the control of the administrators, with the exception of submission of network print jobs which is always allowed. Users are permitted to access any TOE functionality that has a corresponding access control (see section 7.1.3 below) configured for "no security".

The I&A process is controlled by security templates that are associated with functions and menus. Each security template specifies two building blocks – one for authentication and the second for authorization. The security template also includes a list of groups that are authorized to perform the function or access the menu that the security template is associated with.

When I&A is necessary, the TOE examines the authentication building block in the security template to determine what authentication mechanism should be used. The general purpose mechanisms supported in the evaluated configuration are Smart Card authentication, Internal Accounts and LDAP+GSSAPI.

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

Upon successful card validation, the TOE forwards the certificate from the card to the configured Kerberos Key Distribution Center (Windows Domain Controller) for validation. If the certificate validation is not successful, an error message is displayed on the touch panel until the current card is removed from the reader. If the certificate validation is successful, the TOE binds the username, account name, email address (all obtained from the LDAP server), and name of the building block used for authentication to the user session for future use. An audit record for the successful authentication is generated.

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

For Internal Accounts, the TOE performs the validation of the username and password against the set of configured Internal Accounts.

For LDAP+GSSAPI, the TOE forwards the username and password to the configured LDAP server for validation (using the configured machine credentials) and waits for the response. If no response is received, the validation is considered to have failed.

For Internal Accounts and LDAP+GSSAPI, if the validation fails because of an invalid password (for a valid username), the count of failed authentication attempts is incremented for that building block and account combination. If the threshold for failed attempts within a time period is reached, then the account is marked as being locked for the configured amount of time to mitigate against brute force password attacks. This information is tracked in memory and is not

maintained across a restart of the TOE. Note that for LDAP+GSSAPI validations, the server may also be enforcing limits on authentication failures. These mechanisms operate independently and are not required to be comparably configured.

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

If validation is successful, the TOE binds the username, password, account name, email address, group memberships (for Internal Accounts only) and name of the building block used for authentication to the user session for future use (only the username and group memberships are security attributes). An audit record for the successful authentication is generated.

The user session is considered to be active until the user explicitly logs off, removes the card or the administrator-configured inactivity timer for sessions expires. If the inactivity timer expires, an audit record is generated.

7.1.2.1 Backup Password

The Backup Password mechanism allows an administrator to access the Security Menu regardless of the access controls configured for it. When a user attempts to access the Security Menu, the authentication prompt displays a selection that enables a user to authenticate with the Backup Password instead of the method that normally secures this menu. This function may be necessary under unusual circumstances, such as when communication with the LDAP server is not operational.

If the correct Backup Password is supplied, the administrator is considered to be successfully authenticated and authorized for access to the Security Menu (only). A "Successful Authentication" audit record is generated. If an incorrect Backup Password is supplied, an error message is displayed, an audit record is generated, and then the display is returned to the previous screen.

If an invalid password is supplied, the count of failed authentication attempts for the Backup Password is incremented. If the threshold for failed attempts within a time period is reached, then the Backup Password is marked as being locked for the configured amount of time to mitigate against brute force password attacks. This information is tracked in memory and is not maintained across a restart of the TOE.

The Backup Password mechanism may be disabled by an authorized administrator.

7.1.2.2 Active Directory

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

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

7.1.3 Access Control

Access control validates the user access request against the authorizations configured by administrators for specific functions. On a per-item basis, authorization may be configured as "disabled" (no access), "no security" (open to all users), or restricted (via security templates) (some items do not support all three options). Authorization may be configured for the following items:

Table 24 - Access Control Items

Item	Description	Comment
Allow Flash Drive Access	Controls whether USB interfaces may be used for print operations	Must be disabled in the evaluated configuration
App [x]	Controls the execution of eSF and LDD profiles that specify using one of these slots	Access must be restricted to authorized users in the evaluated configuration
Apps Configuration	Controls access to the Applications link (and all sublinks) via the Web page	Access must be disabled or restricted to authorized administrators in the evaluated configuration
Cancel Jobs at the device	Controls access to the functionality to cancel jobs via the touch panel.	Access must be restricted to authorized users in the evaluated configuration
Change Language	Controls access to the Change Language button on the Home screen (when displayed); this button is NOT displayed by default but a user can activate it via the "General Settings Menu"	Any authorization option may be configured
Color Dropout	Controls a user's ability to activate the Color Dropout functionality as part of a job; if protected and the user fails to authenticate, then the device DOES NOT use the color dropout functionality in the job	Any authorization option may be configured
Configuration File Import/Export	Controls the ability to import and export settings and security configuration files	Access must be disabled or restricted to authorized administrators in the evaluated configuration
Configuration Menu (and submenus)	Controls access to the Configuration Menu via the front panel	Must be disabled in the evaluated configuration
Create Bookmarks at the device	Controls access to the Delete Bookmark, Create Bookmark, and Create Folder buttons from both the bookmark list screen and from the individual bookmark screen; unless disabled, all users (regardless of their credentials) can search and print bookmarks	Must be disabled in the evaluated configuration
Create Bookmarks Remotely	Controls access to the Delete Bookmark, Create Bookmark, and Create Folder buttons from both the bookmark list screen and from the individual bookmark screen; unless disabled, all users (regardless of their credentials) can search and print bookmarks	Must be disabled in the evaluated configuration
Firmware Updates	Controls a user's ability to update the device's firmware code via the network	Must be disabled in the evaluated configuration

Item	Description	Comment
Held Jobs Access	Controls access to the Held jobs menu if the "Secure Held Print Jobs" eSF application is not installed	Must be disabled in the evaluated configuration
Network/Ports Menu at the device (and submenus)	Controls access to the Network/ Ports Menu via the Administration Menus	Access must be restricted to authorized administrators in the evaluated configuration
Network/Ports Menu Remotely	Controls access to the Network/ Ports Menu via the web	Access must be restricted to authorized administrators in the evaluated configuration
New Apps	Controls access to configuration parameters for apps subsequently added to the device.	Access must be restricted to authorized administrators in the evaluated configuration
Option Card Configuration at the device	Controls a user's ability to access the "Option Card Menu" that displays menu nodes associated with installed DLEs	Access must be restricted to authorized administrators in the evaluated configuration
Option Card Configuration Remotely	Controls a user's ability to access the "Option Card Menu" via the web	Access must be restricted to authorized administrators in the evaluated configuration
Paper Menu at the device (and submenus)	Controls access to the Paper Menu via the Administration Menus	Any authorization option may be configured
Paper Menu Remotely	Controls access to the Paper Menu via the web	Any authorization option may be configured
PJL Device Setting Changes	When "Disabled", prohibits any changes to system settings via PJL operators	Must be disabled in the evaluated configuration
Remote Management	Controls whether or not management functions may be invoked from remote IT systems	Must be disabled in the evaluated configuration
Reports Menu at the device (and submenus)	Controls access to the Reports Menu via the Administration Menus. This includes information about user jobs, which can't be disclosed to non-administrators.	Access must be restricted to authorized administrators in the evaluated configuration
Reports Menu Remotely	Controls access to the Reports Menu via the web	Access must be restricted to authorized administrators in the evaluated configuration
Secure Held Print Jobs	Controls access to the Held Jobs menu if the "Secure Held Print Jobs" eSF application is installed	Access must be restricted to authorized users in the evaluated configuration
Security Menus at the device (and submenus)	Controls access to the Security Menu via the Administration Menus	Access must be restricted to authorized administrators in the evaluated configuration
Security Menu Remotely	Controls access to the Security Menu via the web	Access must be restricted to authorized administrators in the evaluated configuration
Service Engineer Menus at the device (and submenus)	Controls access to any SE menu accessible from the panel, including the Network SE menu	Access must be restricted to authorized administrators in the evaluated configuration
Note that LDAP+GSSAPI and Smart Card authentication may not be used with this access control because the network interface is not operational when these menus are in use

Item	Description	Comment
Service Engineer Menus Remotely	Controls access to any SE menu accessible from the web	Access must be restricted to authorized administrators in the evaluated configuration
Settings Menu at the device (and submenus)	Controls access to the Settings Menu via the Administration Menus	Access must be restricted to authorized administrators in the evaluated configuration
Settings Menu Remotely	Controls access to the Settings Menu via the web	Access must be restricted to authorized administrators in the evaluated configuration
App [x]	Controls the execution of applications that specify using one of these slots	Any authorization option may be configured
Use Profiles	Controls a user's ability to execute any profile	Access must be configured as no security
Web Import/Export Settings	Protects the Import/Export link in the Settings section of the AIO's Web page and all links beneath the Import/Export link	Must be disabled in the evaluated configuration

Authorization is restricted by associating a security template with an item. The security template assigned to each item may be the same or different as the security template(s) assigned to other items. Each security template points to an authentication building block as well as an authorization building block; the two building blocks may be the same or different.

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

When a function is restricted by a security template, the access control function first determines if the user has already authenticated against the building block contained in the security template. If the user authenticated previously (during the current session), the name of the building block used during that authentication process was cached and can be compared to the name of the building block for this security template. If they match, the authentication step is skipped. Otherwise, if an authentication for a different building block was successfully performed during the current session, the username and password cached from that interaction is re-used for this authentication process against the authentication building block for this security template. If no authentication has already been done for this session, the I&A function is performed before access control continues.

Further access control processing is dependent on the type of authorization building block contained in the security template.

7.1.3.1 Internal Account Building Blocks

The set of groups configured for the Internal Account (and bound to the session during the I&A function) is compared to the set of groups included in the security template. If there are any common groups in those sets, the access control check is satisfied and the user is granted access to the requested function.

7.1.3.2 LDAP+GSSAPI and Smart Card Authentication Client Building Blocks

For each group specified in the authorization building block, the LDAP server is queried to determine if the user is a member of the group. If the user is a member of any of those groups, the access control check is satisfied and the user is granted access to the requested function.

7.1.3.3 Common Processing

The information in this section applies to all types of building blocks.

If the access control check fails for an operation, a message is displayed then the display is returned to the previous screen.

An audit record is generated with the result of the access control check.

7.1.3.4 Function Access Control

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

Table 25 - TOE Function Access Control SFP Rules

Object	Access Control Rules	Configuration Parameter Rules
F.PRT	Network print jobs can always be submitted. The job is held until released by a user who is a member of an authorized group for the Secure Held Print Jobs access control and has the same userid as was specified in the SET USERNAME PJL statement. Network print jobs without a PJL SET USERNAME statement are automatically deleted after the expiry period for held jobs.	Allowed
F.SMI	Print jobs received via the network interface may not be transmitted back out the network interface. Input via the touch panel is not transmitted out the network interface (other than audit records transmitted to the configured Syslog server).	n/a

7.1.3.4.1 Printing

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

7.1.3.5 Postscript Access Control

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

7.1.4 Management

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

The following sections describe the management capabilities provided and are organized by the administrator menu structure available via the touch panel.

7.1.4.1 Reports Menu

The Reports menu provides the ability to print (view) the settings from other menu items. This information must be restricted to authorized administrators.

7.1.4.2 Network/Ports Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 26 - Network/Ports Menu TSF Data

Item	Description	Comments
Network Port	Defines the parameters required for the TOE to communicate via the standard network port	Required in the evaluated configuration
Enable HTTP Server	Enables HTTP(S) server on the TOE	Must be enabled in the evaluated configuration
USB Buffer	Disables all activity via the USB port	Must be disabled in the evaluated configuration

7.1.4.3 Security Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 27 - Security Menu TSF Data

Item	Description	Comments
Edit Backup Password - Use Backup Password	Enables access to the Security Menu via the Backup Password	Only appears if backup password exists. Enabling the backup password is optional.

Item	Description	Comments
Edit Backup Password - Password	Specifies the Backup Password	The TOE requires passwords to be a minimum of 8 characters, with no composition rules. Operational guidance directs administrators to use the following composition rules when specifying passwords: at least one upper case letter, one lower case letter, and one non-alphabetic character; no dictionary words or permutations of the username
Edit Building Blocks - Internal Accounts - General Settings - Required User Credentials	User ID and password (*) User ID	"User ID and password" is required in the evaluated configuration
Edit Building Blocks - Internal Accounts - General Settings - Groups	Defines the groups that may be associated with users, Internal Account building blocks, and security templates (using Internal Accounts)	Required if Internal Account building blocks are used
Edit Building Blocks - Internal Accounts – Manage Internal Accounts	Defines the account name, username, password, email address, and associated groups for each internal account	The TOE requires passwords to be a minimum of 8 characters, with no composition rules. Operational guidance directs administrators to use the following composition rules when specifying passwords: at least one upper case letter, one lower case letter, and one non-alphabetic character; no dictionary words or permutations of the username
Edit Building Blocks - Simple Kerberos Setup - KDC Address, KDC Port, and Realm	Defines how to communicate with the KDC	Required if LDAP+GSSAPI or Smart Card is being used since they use a Kerberos Building Block in order to define the parameters for communication with the KDC
Edit Building Blocks - LDAP+GSSAPI	Defines how to communicate with the LDAP/AD server and (optionally) restrict the groups and users that will match the query	Required if LDAP+GSSAPI is being used to define the LDAP server to be used
Edit Building Blocks - LDAP+GSSAPI – Certificate	default (*) Certificate	The evaluated configuration requires the default certificate if SSL/TLS is selected in the building block.
Edit Building Blocks - LDAP+GSSAPI – Device Credentials	Distinguished username and password to be used when performing LDAP queries	Required in the evaluated configuration
Edit Building Blocks – Active Directory	Defines parameters to join an Active Directory Domain. Upon joining, machine credentials are generated and an LDAP+GSSAPI Building Block is automatically generated with the parameters for the Domain	Optionally used to automatically generate an LDAP+GSSAPI Building Block.
Access Controls	Specifies whether access is no security, disabled, or restricted for each item (see the Access Control security function for the list of items)	Refer to the Access Control security function for requirements on access controls

Item	Description	Comments
Login Restrictions	The "Login failures" value determines how many failed authentications (local OR remote) are allowed within the "Failure time frame" value before the offending User Name is prevented from accessing any function protected with the same building block (e.g. LDAP, Kerberos, etc.) for the duration of the "Lockout time" value. The value of "Panel Login Timeout" determines how long the operator panel can remain idle on the Home screen before the user is logged off automatically.	Any configuration options may be configured. The lockout function is always enabled and any settings within the allowed range will result in a configuration with adequate security against brute force password attacks.
Security Reset Jumper	No Effect No Security (*) Reset to Defaults	"No Security" preserves all of the building blocks and templates that a user has defined, but resets each access control to its factory default security level. "Reset to Defaults" deletes all building blocks and templates that a user has defined and resets each access control to its factory default security level.
LDAP Certificate Verification	Demand (*) Try Allow Never	"Demand!" must be configured in the evaluated configuration
Enable Audit	Determines if the device records events via the remote syslog Yes No (*)	Any configuration options may be configured.
Enable Remote Syslog	Determines if the device transmits logged events to a remote server Yes No (*)	"Yes" must be specified in the evaluated configuration
Remote Syslog parameters	Defines the communication to the remote syslog system	Must be configured in the evaluated configuration.
Date and Time parameters	Controls whether the time is tracked internally or from a remote NTP server	Must be configured for either local or remote operation so that the TOE can provide timestamps in audit records
Held Print Job Expiration Timer	Specifies the maximum amount of time a print job is held while waiting for a user to release it for printing Off 1 hour 4 hours 24 hours 1 week	Any configuration option may be configured.

When an Internal Account is defined, initially no groups are associated with it. The TOE limits the specification of group memberships to defined groups. If a group is associated with any security templates, the group may not be deleted.

7.1.4.4 Settings Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 28 - General Settings Menu TSF Data

Item	Description	Comments
USB Drive	Display (*) Do not display	Must be set to "Do not display" in the evaluated configuration

7.1.4.4.1 Print Settings/Setup Settings Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 29 - Print Settings/Setup Settings Menu TSF Data

Item	Description	Comments
Job Waiting	On Off (*)	Any configuration option may be specified

7.1.4.5 Security Reset Jumper

The security reset jumper provides an alternate mechanism to manage some TSF data. The TOE contains a hardware jumper that can be used to:

- erase all security templates, building blocks, and access controls that a user has defined (i.e. the factory default configuration); OR

- force the value of each function access control to "No Security" (all security templates and building blocks are preserved but not applied to any function).

Administrators can secure the hardware containing the jumper with a Kensington lock. Or, to completely negate the effects of a jumper reset, an authorized administrator can configure the TOE to take no action based upon the jumper, effectively disabling this mechanism. Authorized administrators use the same configuration parameter to determine which of the two actions listed above is performed (if the mechanism is not disabled).

To perform a jumper reset operation, an administrator:

1. powers the device off;

2. removes the Kensington lock from the card cage;

3. removes the small plastic piece that covers a pair of the jumper's pins;

4. replaces the plastic piece so that it covers the pins adjacent to its original position;

5. replaces and secures the Kensington lock on the card cage;

6. powers the device on.

The movement of the plastic piece from position A to position B on the jumper triggers the reset, not the specific positions. When the TOE is powered on, it labels the current position of the plastic piece as the "home" position. If, at the next power on or reset, the TOE detects that the plastic piece has moved from its previous "home" position to the "other" position, then it performs the jumper reset operation. After performing the operation, the TOE also relabels the "other" position as the "home" position.

7.1.5 D.DOC Wiping

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

7.1.6 Secure Communications

IPSec with ESP is required for all network datagram exchanges with remote IT systems. IPSec provide confidentiality, integrity and authentication of the endpoints. Supported encryption options for ESP are TDES and AES. SHA is supported for HMACs.

ISAKMP and IKE are used to establish the Security Association (SA) and session keys for the IPSec exchanges. Diffie-Hellman is used for IKEv1 Key Derivation Function, using Oakley Groups 2, 14, 15, 17 or 18. This session key is stored in RAM. During the ISAKMP exchange, the TOE requires the remote IT system to provide a certificate and the RSA signature for it is validated.

If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded.

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

All session keys are stored in dynamic RAM. The TOE zeroizes the session keys by overwriting once with zeros when the sessions are terminated.

7.1.7 Self Test

During initial start-up, the TOE performs self tests on the hardware. The integrity of the security templates and building blocks is verified by ensuring that all the security templates specified in access controls exist and that all building blocks referenced by security templates exist.

If any problems are detected with the hardware, an appropriate error message is posted on the touch screen and operation is suspended. If a problem is detected with the integrity of the security templates or building blocks, the data is reset to the factory default, an audit log record is generated, an appropriate error message is posted on the touch screen, and further operation is suspended. In this case, a system restart will result in the system being operational with the factory default settings for the data.

8. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 2.

8.1 TOE Type Consistency

Both the PP and the TOE describe Hard Copy Devices.

8.2 Security Problem Definition Consistency

This ST claims demonstrable conformance to the referenced PP as augmented by Attachment A of *CCEVS Policy Letter #20* dated 15 November 2010.

All of the assumptions, threats, and organizational security policies of the PP are included in the ST.

8.3 Security Objectives Consistency

This ST claims demonstrable conformance to the referenced PP as augmented by Attachment A of *CCEVS Policy Letter #20* dated 15 November 2010.

All of the security objectives for the TOE and the operational environment (IT and non-IT) of the PP are included in the ST. The following additional security objectives are included in the ST:

1. O.I&A
2. O.MANAGE
3. O.TIME_STAMP
4. OE.I&A
5. OE.TIME_STAMP

Therefore, the ST is more restrictive than the PP.

8.4 Security Functional Requirements Consistency

This ST claims demonstrable conformance to the referenced PP as augmented by Attachment A of *CCEVS Policy Letter #20* dated 15 November 2010.

All of the SFRs from the claimed SFR packages are included in the ST with any fully or partially completed operations from the PP. Any remaining operations have been completed. The following notes apply to conformance of the SFRs in the ST.

1. The auditable events listed in the table with FAU_GEN.1 have been enumerated to match the specific events generated by the TOE. All of the events required by the PP are represented along with additional events.

2. SFRs from the FCS class have been added to the ST to address cryptographic functionality for IPSec, which are additions to the security functionality required by the PP.

3. FDP_ACC.1(a) and FDP_ACF.1(a) have been integrated with the individual instances of FDP_ACC.1 and FDP_ACF.1 from the applicable SFR packages of the PP into a single instance of FDP_ACC.1 and FDP_ACF.1 (still named Common Access Control SFP) that addresses all of the access control policies.

4. FIA_AFL.1 has been added to the ST to address to address authentication failure handling, which is an addition to the security functionality required by the PP.

5. FIA_UAU.7 has been added to the ST to address to address protected authentication feedback, which is an addition to the security functionality required by the PP.

6. FMT_MSA.1(a) and FMT_MSA.1(b) from the PP were combined into a single instance of FMT_MSA.1 since all the completed operations were identical.

7. FMT_MSA.3(a) and FMT_MSA.3(b) from the PP were combined into a single instance of FMT_MSA.3 since all the completed operations were identical.

8. FMT_MTD.1(a) and FMT_MTD.1(b) from the PP were combined into a single instance of FMT_MTD.1. Users (U.NORMAL) do not have any access to TSF data, and it was necessary to provide permission-level granularity of the administrator role for various TSF data access. Given these conditions, it was simpler to combine the instances of FMT_MTD.1 in the ST.

9. For FMT_SMR.1, the TOE provides greater granularity of roles based on individual permissions that is required by the PP. The permission-based description has been provided in the ST, and an application note with the SFR defines the relationship between those permissions and the roles defined by the PP.

10. FMT_MOF.1 has been added to the ST to address administrator privileges for enabling and disabling security-relevant functionality.

11. The instance of the FAU_GEN.1 in the SMI package has been integrated with the instance of FAU_GEN.1 in the common requirements.

8.5 Security Assurance Requirements Consistency

The ST assurance claims are identical to the assurance claims of the PP.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat, policy and assumption is addressed by a security objective.

The following table identifies for each threat, policy and assumption, the security objective(s) that address it.

Table 30 - Threats, Policies and Assumptions to Security Objectives Mapping

	O.AUDIT.LOGGED	O.CONF.NO_ALT	O.CONF.NO_DIS	O.DOC.NO_ALT	O.DOC.NO_DIS	O.FUNC.NO_ALT	O.INTERFACE.MANAGED	O.I&A	O.MANAGE	O.PROT.NO_ALT	O.SOFTWARE.VERIFIED	O.TIME_STAMP	O.USER.AUTHORIZED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.AUDIT.REVIEWED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT_STORAGE.PROTECTED	OE.I&A	OE.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.TIME_STAMP	OE.USER.AUTHORIZED	OE.USER.TRAINED
A.ACCESS.MANAGED																					X			
A.ADMIN.TRAINING														X										
A.ADMIN.TRUST															X									
A.USER.TRAINING																								X
T.CONF.ALT		X						X					X						X				X	
T.CONF.DIS			X					X					X						X				X	
T.DOC.ALT				X				X					X						X				X	
T.DOC.DIS					X			X					X						X				X	
T.FUNC.ALT						X		X					X						X				X	
T.PROT.ALT								X		X			X						X				X	
P.AUDIT.LOGGING	X											X				X	X	X				X		
P.INTERFACE.MANAGEMENT							X													X				
P.SOFTWARE.VERIFICATION											X													
P.USER.AUTHORIZATION								X	X				X						X				X	

9.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 31 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.CONF.ALT	O.CONF.NO_ALT – The objective addresses the threat by requiring the TOE to protect against unauthorized alteration of TSF Confidential Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.CONF.DIS	O.CONF.NO_DIS - The objective addresses the threat by requiring the TOE to protect against unauthorized disclosure of TSF Confidential Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.DOC.ALT	O.DOC.NO_ALT - The objective addresses the threat by requiring the TOE to protect against unauthorized alteration of User Document Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.DOC.DIS	O.DOC.NO_DIS - The objective addresses the threat by requiring the TOE to protect against unauthorized disclosure of User Document Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.FUNC.ALT	O.FUNC.NO_ALT - The objective addresses the threat by requiring the TOE to protect against unauthorized alteration of User Function Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.PROT.ALT	O.PROT.NO_ALT - The objective addresses the threat by requiring the TOE to protect against unauthorized alteration of TSF Protected Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.

9.1.2 Rationale Showing Policies to Security Objectives

The following table describes the rationale for the policy to security objectives mapping.

Table 32 - Policies to Security Objectives Rationale

P.TYPE	Security Objectives Rationale
P.AUDIT.LOGGING	O.AUDIT.LOGGED – The objective addresses the first part of the policy by requiring the TOE to generate audit records for TOE usage and security-relevant events, and to protect these records while they are inside the TSC. O.TIME_STAMP – The objective supports the policy by requiring the TOE to provide time stamps for the audit records when time is being tracked internally. OE.AUDIT.REVIEWED – The objective addresses the audit review portion of the policy by requiring timely review of the generated audit records. OE.AUDIT_ACCESS.AUTHORIZED – The objective supports the policy by requiring the operational environment to make the audit records available to authorized personnel only. OE.AUDIT_STORAGE.PROTECTED - The objective supports the policy by requiring the operational environment to protect the stored audit records from unauthorized access. OE.TIME_STAMP - The objective supports the policy by requiring the TOE to provide time stamps for the audit records when time is being supplied externally.
P.INTERFACE.MANAGEMENT	O.INTERFACE.MANAGED – The objective addresses the policy by requiring the TOE to enforce access to and usage of the TOE interfaces within the TSC. OE.INTERFACE.MANAGED – The objective addresses the policy by requiring the operational environment to control access to the TOE interfaces within the operational environment.
P.SOFTWARE.VERIFICATION	O.SOFTWARE.VERIFIED – The objective restates the policy.
P.USER.AUTHORIZATION	O.I&A and OE.I&A – The objectives help address the policy by requiring I&A mechanisms so that user authorizations may be restricted for users. O.MANAGE – The objective addresses the policy by requiring the TOE to provide management functions to administrators for configuration of user authorizations. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the policy by requiring authorizations to be specified for users.

9.1.3 Rationale Showing Assumptions to Environment Security Objectives

The following table describes the rationale for the assumption to security objectives mapping.

Table 33 - Assumptions to Security Objectives Rationale

A.TYPE	Security Objectives Rationale
A.ACCESS.MANAGED	OE.PHYSICAL.MANAGED – The objective addresses the assumption by requiring the TOE to be located in an area that restricts physical access.
A.ADMIN.TRAINING	OE.ADMIN.TRAINED – The objective restates the assumption.
A.ADMIN.TRUST	OE.ADMIN.TRUSTED – The objective addresses the assumption by requiring trust to be established in the administrators.
A.USER.TRAINING	OE.USER.TRAINED – The objective restates the assumption.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 34 - SFRs to Security Objectives Mapping

	O.AUDIT.LOGGED	O.CONF.NO_ALT	O.CONF.NO_DIS	O.DOC.NO_ALT	O.DOC.NO_DIS	O.FUNC.NO_ALT	O.INTERFACE.MANAGED	O.I&A	O.MANAGE	O.PROT.NO_ALT	O.SOFTWARE.VERIFIED	O.TIME_STAMP	O.USER.AUTHORIZED
FAU_GEN.1	X											X	
FAU_GEN.2	X												
FCS_CKM.1		X	X	X	X	X				X			
FCS_CKM.4		X	X	X	X	X				X			
FCS_COP.1		X	X	X	X	X				X			
FDP_ACC.1(A)				X	X	X	X			X			X
FDP_ACC.1(B)				X	X		X			X			X
FDP_ACF.1(A)				X	X	X	X			X			X
FDP_ACF.1(B)				X	X		X			X			X
FDP_RIP.1					X								
FIA_AFL.1								X					
FIA_ATD.1								X					
FIA_UAU.1								X					X
FIA_UAU.7								X					
FIA_UID.1								X					X
FIA_USB.1								X					X
FMT_MOF.1		X	X						X				X
FMT_MSA.1		X	X						X				X
FMT_MSA.3									X				
FMT_MTD.1		X	X						X				X
FMT_SMF.1									X				
FMT_SMR.1									X				
FPT_FDI_EXP.1							X						
FPT_STM.1												X	
FPT_TST.1											X		
FTA_SSL.3									X				
FTP_ITC.1		X	X	X	X	X				X			

The following table provides the detail of TOE security objective(s).

Table 35 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDIT.LOGGED	FAU_GEN.1 addresses the objective by requiring the TOE to generate audit records for TOE usage and security relevant events. FAU_GEN.2 helps address the objective by requiring the audit records to include information associating a user with each event (if applicable).
O.CONF.NO_ALT	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 support the objective by requiring the TOE to provide key management and cryptographic functions to protect management interactions during network transmission. FMT_MOF.1 specifies the rules for managing the behaviour of security-relevant functions, which is done by altering TSF Confidential Data and should only be accessed by authorized administrators. FMT_MSA.1 specifies the rules for managing user security attributes used in user data access control decisions, which is done by altering TSF Confidential Data and should only be accessed by authorized administrators. FMT_MTD.1 specifies the rules for altering TSF Confidential Data. FTP_ITC.1 addresses the objective by requiring the TOE to provide trusted channels for the exchange of management traffic across the network.
O.CONF.NO_DIS	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 support the objective by requiring the TOE to provide key management and cryptographic functions to protect management interactions during network transmission. FMT_MOF.1 specifies the rules for managing the behaviour of security-relevant functions, which includes displaying TSF Confidential Data and should only be accessed by authorized administrators. FMT_MSA.1 specifies the rules for managing user security attributes used in user data access control decisions, which includes displaying TSF Confidential Data and should only be accessed by authorized administrators. FMT_MTD.1 specifies the rules for displaying TSF Confidential Data. FTP_ITC.1 addresses the objective by requiring the TOE to provide trusted channels for the exchange of management traffic across the network.
O.DOC.NO_ALT	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 support the objective by requiring the TOE to provide key management and cryptographic functions to protect the document data while transferred across the network. FDP_ACC.1(A) and FDP_ACC.1(B) specify the subjects, objects and operations that are controlled regarding User Document Data that must be protected for unauthorized alteration. FDP_ACF.1(A) and FDP_ACF.1(B) specify the security attributes and rules used to determine whether access is permitted. FTP_ITC.1 addresses the objective by requiring the TOE to provide trusted channels for the exchange of D.DOC across the network.
O.DOC.NO_DIS	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 support the objective by requiring the TOE to provide key management and cryptographic functions to protect the document data while transferred across the network. FDP_ACC.1(A) and FDP_ACC.1(B) specify the subjects, objects and operations that are controlled regarding User Document Data that must be protected for unauthorized disclosure. FDP_ACF.1(A) and FDP_ACF.1(B) specify the security attributes and rules used to determine whether access is permitted. FDP_RIP.1 supports the objective by requiring the TOE to make unavailable any user document data when the RAM buffer holding the data is released. FTP_ITC.1 addresses the objective by requiring the TOE to provide trusted channels for the exchange of D.DOC across the network.

Security Objective	SFR and Rationale
O.FUNC.NO_ALT	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 support the objective by requiring the TOE to provide key management and cryptographic functions to protect the function data while transferred across the network. FDP_ACC.1(A) specifies the subjects, objects and operations that are controlled regarding functions. FDP_ACF.1(A) specifies the security attributes and rules used to determine whether access is permitted. FTP_ITC.1 addresses the objective by requiring the TOE to provide trusted channels for the exchange of D.FUNC across the network.
O.INTERFACE.MANAGED	FDP_ACC.1(A), FDP_ACC.1(B) and FDP_ACC.1(C) specify the subjects, objects and operations that are controlled regarding all TOE interfaces. FDP_ACF.1(A), FDP_ACF.1(B) and FDP_ACF.1(C) specify the security attributes and rules used to determine whether access is permitted. FPT_FDI_EXP.1 specifies that the TOE restrict the flow of information between the network and fax interfaces.
O.I&A	FIA_AFL.1 supports the objective by requiring the TOE to lock accounts that experience an excessive number of failed authentication attempts, thereby providing protection from brute force password attacks. FIA_ATD.1 specifies the attributes associated with users, including information about failed authentication attempts. FIA_UAU.1 requires the TOE to provide I&A using Internal Accounts and the Backup Password. FIA_UAU.7 protects the confidentiality of passwords by specifying that only asterisks are echoed during password entry. FIA_UID.1 requires the TOE to provide I&A using Internal Accounts and the Backup Password. FIA_USB.1 specifies the attributes bound to a session upon successful completion of the I&A process.
O.MANAGE	FMT_MOF.1 specifies the rules for administrator access to the listed functions. FMT_MSA.1 specifies the rules for management of the security attributes used in the access control decisions for user data. FMT_MSA.3 requires the TOE to impose restrictive default values for security attributes in all cases. FMT_MTD.1specifies the rules for management of TSF data. FMT_SMF.1 specifies the management functions that the TOE provides and controls access to. FMT_SMR.1 specifies the roles (via user permissions) supported by the TOE. FTA_SSL.3 requires the TOE to automatically terminate idle sessions to mitigate against users taking advantage of existing sessions to gain unauthorized access.
O.PROT.NO_ALT	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 support the objective by requiring the TOE to provide key management and cryptographic functions to protect the management data while transferred across the network. FDP_ACC.1(A) and FDP_ACC.1(B) specify the subjects, objects and operations that are controlled regarding TSF Protected Data that must be protected for unauthorized alteration. FDP_ACF.1(A) and FDP_ACF.1(B) specify the security attributes and rules used to determine whether access is permitted. FTP_ITC.1 addresses the objective by requiring the TOE to provide trusted channels for the exchange of management traffic across the network.
O.SOFTWARE.VERIFIED	FPT_TST.1 addresses the objective by requiring the TOE to validate the TSF data for security templates and building blocks.

Security Objective	SFR and Rationale
O.TIME_STAMP	FPT_STM.1 requires the TOE to provide a reliable time source when time is configured to be supplied internally.
O.USER.AUTHORIZED	FIA_UID.1 and FIA_UAU.1 requires the TOE to successfully complete the I&A process before allowing users to perform anything other than the specified functions. FIA_USB.1 specifies the attributes bound to a sessions (and used in access control decisions) upon successful I&A. The security policies defined in FDP_ACC.1(A), FDP_ACC.1(B), FDP_ACF.1(A), FDP_ACF.1(B), FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 are required to be enforced by the TOE based on the security attributes bound to the subject (acting on behalf of the authenticated user).

9.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented with ALC_FLR.2 from part 3 of the Common Criteria.

9.3 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 36 - SFRs to TOE Security Functions Mapping

	Audit Generation	I&A	Access Control	Management	D.DOC Wiping	Secure Communication	Self Test
FAU_GEN.1	X						
FAU_GEN.2	X						
FCS_CKM.1						X	
FCS_CKM.4						X	
FCS_COP.1					X	X	
FDP_ACC.1(A)			X				
FDP_ACC.1(B)			X				

	Audit Generation	I&A	Access Control	Management	D.DOC Wiping	Secure Communication	Self Test
FDP_ACF.1(A)			X				
FDP_ACF.1(B)			X				
FDP_RIP.1					X		
FIA_AFL.1		X					
FIA_ATD.1		X					
FIA_UAU.1		X					
FIA_UAU.7		X					
FIA_UID.1		X					
FIA_USB.1		X					
FMT_MOF.1			X	X			
FMT_MSA.1			X	X			
FMT_MSA.3				X			
FMT_MTD.1			X	X			
FMT_SMF.1				X			
FMT_SMR.1				X			
FPT_FDI_EXP.1			X				
FPT_STM.1	X						
FPT_TST.1							X
FTA_SSL.3		X					
FTP_ITC.1						X	

Table 37 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1	Audit Generation addresses the SFR by specifying the audit event records that are generated and the content of the records.
FAU_GEN.2	Audit Generation addresses the SFR by specifying that the associated Username (if applicable) is included in audit event records.
FCS_CKM.1	Secure Communications requires generation of a certificate with an RSA public-private key pair.
FCS_CKM.4	Secure Communication requires zeroization of the session keys obtained by DH IKEv1 Key Derivation Function to be zeroized when the sessions terminate.
FCS_COP.1	Secure Communication requires the TOE to support TDES and AES for encryption, AES and SHA for HMAC, RSA signatures, Diffie Hellman for IKEv1 Key Derivation Function, and a deterministic random bit generator.
FDP_ACC.1(A)	Access Control specifies the access controls placed on the user operations (objects) performed by users to access user data in the TSC.
FDP_ACC.1(B)	Access Control specifies the access controls placed on the user operations (objects) performed by users to access user data in the TSC.
FDP_ACF.1(A)	Access Control specifies the access controls placed on the user operations (objects) performed by users to access user data in the TSC.
FDP_ACF.1(B)	Access Control specifies the access controls placed on the user operations (objects) performed by users to access user data in the TSC.

SFR	SF and Rationale
FDP_RIP.1	D.DOC Wiping requires the TOE to overwrite RAM buffers upon their release that contain user data from incoming print jobs.
FIA_AFL.1	Identification and Authentication requires the TOE to track failed login attempts for all authentication mechanisms. The limit on failed attempts that triggers an account lock is specified via the Login Restrictions TSF data.
FIA_ATD.1	Identification and Authentication requires the TOE to maintain the Username, Password, and Associated Groups security attributes for Internal Accounts and the Backup Password; and the failed authentication security attributes for all users.
FIA_UAU.1	Identification and Authentication requires the TOE to prevent access to restricted functions before the I&A process is successfully completed. Printing is never a restricted function; other functions may be restricted through access controls or enabling/disabling specific functions such as incoming faxes. The TOE is solely responsible for I&A for Internal Accounts and the Backup Password.
FIA_UAU.7	Identification and Authentication requires the TOE to echo asterisks when a password is being entered for the I&A process for all mechanisms.
FIA_UID.1	Identification and Authentication requires the TOE to prevent access to restricted functions before the I&A process is successfully completed. Printing is never a restricted function; other functions may be restricted through access controls or enabling/disabling specific functions such as incoming faxes. The TOE is solely responsible for I&A for Internal Accounts and the Backup Password.
FIA_USB.1	Identification and Authentication requires the TOE to bind the Username and Password supplied during I&A with the subject upon successful I&A. The TOE also binds the list of associated groups (for Internal Accounts) and the building block name used for I&A.
FMT_MOF.1	Management requires the TOE to provide the management capabilities specified in the table to the administrators that satisfy the access controls associated with the menus that control those functions. Access Control specifies that access be restricted and states the required configuration in the evaluated configuration.
FMT_MSA.1	Management requires the TOE to provide the management capabilities for Usernames and Group memberships to the administrators that satisfy the access controls associated with the menus that control access to the data items. Access Control specifies that access be restricted and states the required configuration in the evaluated configuration.
FMT_MSA.3	Management requires the TOE to initially associate no group memberships with Internal Accounts.
FMT_MTD.1	Management requires the TOE to provide the management capabilities specified in the table to the administrators that satisfy the access controls associated with the menus that control access to the data items. Access Control specifies that access be restricted and states the required configuration in the evaluated configuration.
FMT_SMF.1	Management requires the TOE to provide capabilities to manage the specified functions.
FMT_SMR.1	Management requires the TOE to maintain the two specified roles. Administrators are any users authorized access to management functionality, while normal users are all the other defined users.
FPT_FDI_EXP.1	Access Control requires the TOE to prevent data from being forwarded from the network interface or the touch panel to the network interface.

SFR	SF and Rationale
FPT_STM.1	Audit Generation requires the TOE to provide time stamps for audit records when the TOE is configured for internal time.
FPT_TST.1	Self Test requires the TOE to perform tests on the hardware and validate the security templates and building blocks on each power up and reset.
FTA_SSL.3	Identification and Authentication states that sessions are automatically terminated by the TOE when the Home menu is not accessed within the configured timeout period.
FTP_ITC.1	Secure Communication requires the TOE to use a trusted channel for network communication with all remote IT systems.